A publication of ISCA*:
International Society for Computers
and Their Applications

INTERNATIONAL JOURNAL OF COMPUTERS AND THEIR APPLICATIONS

TABLE OF CONTENTS

***"International Journal of Computers and Their Applications is Peer Reviewed".**

Volume 29, No. 4, December 2022 **ISSN 1076-5204**

International Journal of Computers and Their Applications

A publication of the International Society for Computers and Their Applications

ISCA Headquaters • 278 Mankato Ave, #220, Winona, Minnesota 55987, USA
Phone 507-458-4517 • Email isca@isca-hq.org • URL: http://www.isca-hq.org

Guest Editor's Editorial

This Special Issue of IJCA contains six selected papers submitted by authors from five countries including Egypt, USA, Indonesia, Jordan and North Macedonia. Topics of them focus on algorithm complexity, cryptography technique, and their applications.

Each paper was reviewed by at least two editorial board members and additional reviewers, judging the originality, scientific contributions, significance of results, applications and writing quality. The work contributes to the state-of-the-art advancement of today's information technology and software engineering development.

As a team of faculty members, graduate student and senior undergraduate student from Southeast Missouri State University, USA, Blake Bleem, Vishwanath Varma Indukuri, Reshmi Mitra and Indranil Roy introduced the framework of CTChain in the paper "*CTChain: blockchain platform for contact tracing and mapping active infections".* The system works as a tool in controlling the spread of infection diseases such as the COVID-19 by collecting, organizing, and generating maps of active infections. The hierarchical network architecture is built by navigating via a cache memory-stored blockchain.

Rania Shaqbou'a, Nedal Tahat, O. Y. Ababneh and Obaida M. Al-Hazaimeh from three universities of Jordan (The Hashemite University, Zarqa University, Al-Balqa Applied University) proposed a novel signature technique in the paper "*Chaotic map and quadratic residue problems-based hybrid signature scheme*". The idea is based on two hard number theory quadratic residue (QR) and chaotic maps (CM). The new method has the advantage of reducing calculation cost, enhanced security and improved productivity.

A group of four co-authors from the South East European University of North Macedonia, Armend Salihu, Halil Scopce, Artan Luma and Jaumin Ajdari, presented their results from algorithm complexity analysis in the paper "*Time complexity analysis for Cullis/Radic and Dodgson's generalized/modified method for rectangular determinants calculations*". They identified the asymptotic time complexity and introduced a combination of the two algorithms as a relatively more efficient approach.

Two Ph.D students and a professor from the University of Indonesia, Delphi Hanggoro, Jauzak Hussaini Windiatmaja and Riri Fitri Sari, investigated algorithms for wireless sensor network in the paper "*Comparative study between aura and clique blockchain-based proof of authority algorithms on wireless sensor network*". Their empirical study compared two permissioned blockchains consensuses Proof-of-Authority algorithms named Aura and Clique and concluded that Aura is more suitable than Clique to apply to wireless sensor networks.

Two professors, Ismail Ababneh and Saad Bani-Mohammad from Al al-Bayt University in Jordan presented their study on time complexity in the paper "*An efficient maximal free submesh detection scheme for space-multiplexing in 2d mesh-connected manycore computers*". The proposed scheme is shown to have quadratic time complexity in the number of free submeshes, whereas the time complexity of the previous such scheme is cubic in this number.

Finally, Shaimaa Haridy, Rasha M. Ismail, Nagwa Badr and Mohamed Hashem from the Ain Shams University of Egypt introduced an enhanced architecture for the ontology development lifecycle in the paper "*The combination of ontology-driven conceptual modeling and ontology matching for building domain ontologies: e-government case study*". The new architecture allows users to complete ontology development tasks by providing guidance for all key activities, from requirement specification to ontology evaluation. As a case study, the design is applied to e-governance domain. The results are encouraging when the produced ontology is compared with 20 existing ontologies from the same domain.

As a guest editor, I would like to express my deepest appreciation for the invitation from Dr. Narayan Debnath, the ISCA director and Dr. Gongzhu Hu the ISCA president, and the great support from Dr. Ajay Bandi, the editor-in-chief of IJCA. I also thank the authors for their contributions, as well as the experts who reviewed the papers submitted to this issue.

More information about ISCA society can be found at http://www.isca-hq.org.

Guest Editor
Wenying Feng, Trent University, Canada

CTChain: Blockchain Platform for Contact Tracing and Mapping Active Infections

Blake Bleem *, Vishwanath Varma Indukuri *, Reshmi Mitra *, Indranil Roy *
Southeast Missouri State University, Cape Girardeau, MO 63701, USA

Abstract

Despite the effectiveness of social isolation and, in particular, contact tracing for infection management, there are a number of drawbacks, including that it is time-consuming, labor-intensive, and adhoc. Following the COVID-19 outbreak, a number of mobile technologies are emerging to combat the inefficiencies of human contact tracing. However, there is a lack of actual, transparent platform design, and the production of maps for active infection, particularly in the state-of-the-art Blockchain technology. In this paper we introduce CTChain, a blockchain-based tool that collects, organizes, and generates maps of active infections to assist public health officials in their work. Utilizing a hierarchical network architecture, a regional map for active infection is built by navigating via a cache memory-stored blockchain. Our architecture continuously filters out outdated infections to produce batches of the most pertinent dynamic regional data, which may be utilized to issue timely health recommendations and temporarily seal off high-infection areas. CTChain's platform can map the active infections across three different parameters: sparse vs densely populated region, number of people in each location, and initial infection rate. We can examine infection transmission and region "popularity" on a per-region basis because of our region handler capabilities. Due to the network's widespread storage of many copies of the chain, our model is safeguarded against single points of failure.

Key Words: Infection containment; blockchain; contact tracing; network design; client-server; active notification; *

1 Introduction

The health and welfare of the global population was severely debilitated with widespread pandemic outbreaks [37] especially due to COVID-19. It began with less than 30 active infections in Wuhan, China in late 2019 due to the new coronavirus SARS-CoV-2. Since then it has spread to 623 million people on a global basis, and 6.5 million have died as a result [7]. The World Health Organization (WHO) designated COVID-19 as a global public health emergency in January 2020, just a few months after the initial outbreak. Highly contagious diseases such as SARS-CoV-2 is typically spread through personal contact between an infected person and a healthy person [3]. According to several studies, the illness is also extremely contagious and can spread through airborne particles, which only accelerates its unchecked spread. Both symptomatic and asymptomatic infected individuals have the potential to spread the virus. According to one study done in Wuhan [26], the incubation period extends from one to fourteen days, therefore the only option to restrict the spread is to quarantine sick people to a single location during that period. Overall, the healthcare system across the entire world has been over-stretched beyond limits to address the extremely precarious aftermaths of the pandemic.

Many nations have implemented Non-Pharmaceutical Intervention (NPI) [19] to stop the spread of the virus in response to this unprecedented global disaster. These measures include closing offices and schools, and even enforcing countrywide lock-downs. Governments throughout the world have been enforcing several drastic measures to prevent any form of social interaction that limits the infection spread. To minimize human contact, complete worldwide lock-downs has been imposed that includes closing statewide and international borders, closing schools and universities, requesting that employees work from home, closing malls and markets, and suspending public gatherings. These preventative measures caused a downward spiralling effect on the economy, which has led to the search for better public health solutions. Health professionals, scientists, engineers, and administrators are compelled to design easy-to-adapt solutions as the entire world is struggling through this "new normal".

Popular NPI technique for social isolation technique called *contact tracing* seeks to locate and monitor individuals who have come in contact with another infected person. To break the chain of transmission, early screening, diagnosis, and treatment is administered to the identified close contacts. To relieve the severe social distancing limits explained earlier most countries have adopted this tracking approach. In particular, the experience in Hong Kong has shown that contact tracing can successfully prevent the spread of COVID-19 by lowering community transmission from undiagnosed cases [21]. However, typical manual contact tracing is completely dependent on one's memory of remembering and sorting the daily (infection) contacts, which can lead to inconsistent data reporting. Moreover, it does not scale effectively once the pandemic has progressed past its early stages owing to the limited number of employees necessary to carry out the operation. Therefore, designing an efficient and secure digital solution is essential for collecting and managing such high volume dynamic data. Using this information public health professionals can effectively handle active cases by

*Email: {bhbleem1s, sindukuri1s, rmitra, iroy}@semo.edu

avoiding crowded settings and socially isolating the patients. Additionally, the town/city/state administration can utilize this data to pinpoint the locations of current active infections and provide public advisories to combat false information.

In this paper, our main objective is to develop an end-to-end complete blockchain based solution that can collect, sort and generate active infection maps to support the work of health officials. Our solution is termed as ***CTChain: Contact Tracing Chain***, as it uses the inherent *Proof of Authority (PoA)* properties of blockchain to process the dynamic infection contact data. It uses several inbuilt smartphone technologies such as Bluetooth and Global Positioning Systems (GPS) to estimate the closeness and length of a person's exposure to others. The *hierarchical network architecture* comprises of three node types: client, hospital and city. The blocks from each node needs are validated by its parent-level as per inherent PoA characteristics. The regional map for active infection is built by traversing through the chain stored in cache memory pool at the hospital node. Our framework continually prunes the outdated infections to create batches of most relevant dynamic regional data, which can be used by health officials to issue timely health advisories.

We are evaluating capability of CTChain to effectively map the active infections across three different parameters: sparse vs densely populated region, number of people in each region, and initial infection rate. We use grid-view to present nine different combinations, which can be used by health officials to model potential scenarios and plan accordingly. We show concrete results that our platform can handle wide variation of infection rates ranging from mild to complex cases in sparsely and densely populated regions. Our 'region handler' allows us to comb through infection spread and region "popularity" on per-region basis. Although past work has showcased the blockchain architecture for privacy needs without meaningful implementation details, *CTChain presents realistic multi-level platform design with the emphasis on region handler for localized infection maps*. Our model is protected from single point of failure as multiple copies of the chain is stored throughout the network. Its open public architecture makes it relevant for multi-modal data storage and sorting for realistic contact tracing.

There are four main sections in this paper. Section 2 discusses the summary of state-of-art about blockchain-based contact tracing solutions. In Section 3, we describe the proposed framework of the hierarchical network design. Section 4 discusses the performance of the proposed method. The research highlights with concluding remarks and future work are presented in Section 5.

2 Related Work

2.1 Contact Tracing Mobile Apps

By expediting disclosure and contact tracing procedures through efficient digital data flow, connectivity tracing, and location monitoring, contact tracing applications can assist with test findings, locating, distancing, and quarantining steps in an effort to stop and halt the spread of the Covid virus. Given the extensive usage of web-based devices, it may be essential to speed up the monitoring of a large population of smartphone users in order to find infectious disease hot-spots practically and immediately [7].

To help public health organizations throughout the world create digital contact tracking tools, Apple and Google together unveiled a new breakthrough for third-party applications for iOS and Android devices[39].The concept is to employ Bluetooth low-energy beaconing technology to keep track of when a device approaches someone using the app to locate and find infections[55]. Given that Google Android and Apple iOS together have the greatest smartphone operating system user base, it is probable that one's approach will be key in how the bulk of contact-tracing applications perform[23]. Since the implementation of lockdown safety measures, many applications, including Healthcode, Covidsafe, Coronawarn, Aarogya setu, and NHS, have been developed to reduce the danger of SARS-CoV-2 transmission. We have compiled information about the different apps that have been used for the cause in the following subsections, organized by country.

2.1.1 United States of America (USA):

The computerized contact tracking project in Virginia comprises 2 million users. One-fourth of the populace has downloaded the state's "Covidwise" app or signed in to get alerts about hazards on their smartphones [6]. Almost 26,000 warnings have been sent out warning people that they were likely exposed to someone possessing COVID-19[53]. COVID Alert NY" offers voluntary, anonymous exposure notifications. You would be notified if you had any kind of close contact with someone who tested positive for COVID-19. Knowing that you could have been exposed allows you to immediately isolate yourself, get checked out, and lower the danger of exposure.[5]. These two programs were among the first contact tracking methods to become well-known in the US [4].

2.1.2 United Kingdom (UK):

Along with the United Kingdom (UK) [22] and the 27 other participating nations that make up the European Union (EU), the European Commission (EC) offered a number of solutions to the COVID contact tracing issue. The most well-known programs among them are "Coronalert" from Belgium, "CoronaMelder" from the Netherlands, "VirusRadar" from Hungary, and "Immuni" from Italy [30].

Notably, "NHS COVID 19" from the UK National Health Services received a ton of favorable feedback from users in the relevant app stores (Apple App Store and Google Play Store)[2].

2.1.3 India:

The "Aarogya Setu" system in India uses contact tracing to keep tabs on everyone you connect with while going about your daily activities[29]. The appropriate parties would be informed

and assertive medical care would be arranged for you if one of them later tested positive for COVID-19 [29].

2.1.4 New Zealand and Australia:

New Zealand's success against COVID-19 at the national level is a fascinating issue for researchers studying pandemic prevention. [12] Prior to officially declaring the pandemic finished in June 2020, New Zealand had just 1,569 cases that had been registered and 22 fatalities, which was the best worldwide epidemic outcome of any nation in the globe. The "NZ COVID Tracer" app offers live statistical data that is considered superior to the competitors, as well as on-location QR codes [8]. Australia's "COVIDSafe" has become an appealing option despite the app's poor performance because of the country's generally low number of instances well before the start of 2022. Their iOS app's ineffective design on occasion resulted in service outages and false positive alarms when requirements were not satisfied [44] .

2.1.5 Singapore and France:

Singapore's contact-tracing app, "Trace-Together" had about one million downloads (20 % of the population), and 16 people were active users at the time of launch. The French contact tracing software Stop-Covid has received 1.9 million downloads across the App Store and the Play Store, and it alone has issued 14 alerts in the first few days of operation.

2.1.6 South Korea and Hong Kong:

The use of contact tracing apps, like the "Corona 100" which seem to be widespread in South Korea, enables public health professionals to reduce the time needed to track a person's movement patterns from roughly 24 hours to roughly 10 minutes, helping the general public stay away from contagious areas. The Hong Kong government required the download of the "StayHomeSafe" app and provided armbands with geo-location automated tracking services that alert agents if wearers violated exclusion zones.

Manufacturing scholars and specialists in Liberal nations have questioned the effectiveness of contact tracing applications in finding and following persons infected with the novel COVID virus. [16]. Technical, privacy and security difficulties have made the applications difficult to use, and it is uncertain whether any of them have had an impact on the global COVID-19 pandemic.

Authors examined an organized mapping of global implementation frameworks and advances, along with a comprehensive study of flaws for each circumstance [34]. In order to support healthcare information decision-making with reference to the UK's current position in COVID-19, the major issues facing Bluetooth-based solutions are clearly identified [14]. Rolling Proximity Identifiers (RPI), which are regularly changing spontaneous pseudonyms, are used in the GAP contact tracking method. A GAP architecture is extremely vulnerable to relay-based wormhole attacks, which may produce bogus contacts and potentially compromise the accuracy of only an app-based contact tracking structure, as well as profiling and potentially de-anonymizing infected individuals. [1]. The results show that the mobile apps [28] were used to monitor self-isolated participants, spot those who weren't wearing masks, determine if they had close contact with an infected person, provide precise time and location of the contact, and evaluate the risk of contracting the disease [41].

Contact tracing is indeed the method of recognizing people who may have been in contact with the infected individual and then gathering additional details about such contacts.[50] Contact tracing, in addition to testing, is a useful technique for decelerating the expansion of COVID-19. It's a basic medical investigator tool designed to keep your family, friends, and local residents safe if you've subjected them to the virus.[20]

Effectiveness-wise, it is yet to be proven that Bluetooth can provide an accurate estimate of range while avoiding a high false alarm rate [33]. The secrecy of those who have been infected is at risk due to the updated decentralized techniques used by several nations, [46]. The privacy of those users is in jeopardy when centralized techniques are used, such as those in France used with ROBERT, especially when a malicious centralized power or a hacker is attempting to attack this control. Furthermore, the centralized method seems to be a preferable option if privacy with reference to authority isn't a concern because it seems to permit the establishment of a system that is more beneficial for epidemiologists and that can safeguard privacy from outside attacks, [11]. Choosing between the centralized and decentralized systems is just as challenging as employing automated contact tracking in the first place because neither strategy offers appropriate privacy protection [54].

The "Contra Corona" methodology provides a cutting-edge, "hybrid" approach to digital contact tracing that protects both the history of the interaction chart and the presence or absence of infectious diseases. By giving away the server's essential tasks to multiple organizations, it may be possible to reduce the degree of confidence in the server-based components[17].

2.2 Contact Tracing with Blockchain

Until a vaccine is created and made accessible for usage, policymakers and governments are having a tough time attempting to stop the rapid spread of the pandemic Covid-19 [43]. Blockchain technology will be used in this situation to securely record every transaction correspondence between users who have networked devices that can access the cloud. In order to use contact tracings, health professionals and the relevant government immediately seek just the blockchain transactional data corresponding to the infected individuals. A crucial public health strategy to stop the spread of the COVID-19 pandemic and other emerging infectious illnesses is contact tracing, according to [28]. However, care is advised when generalizing app usability, particularly in lower middle-income countries, and when addressing issues with data anonymity, privacy, usage, and rights [10].

Because blockchain technologies are decentralized, safe, and highly regulated, many industries have profited from them [38]. They have enormous potential in epidemic circumstances as well. By notifying those who may have been exposed so they may take the necessary measures, contact tracing aids in the prevention of disease spread. Contact tracing systems have some issues with data security, medical privacy, and transparency. Contact tracing hinders patients from getting medicine because they are afraid of data loss and subsequent shame, marginalization, or abuse, according to several research studies[35].

2.2.1 CovidBloc:

The COVID 19 exposure database is implemented by CovidBloc, a contact tracking system that utilizes the Hyperledger Fabric Blockchain Network [42]. A mobile application operating on a Bluetooth-enabled mobile phone, an internet software platform for health authorities, and a backend web service attempting to serve as a storage site for data being gathered make up the CovidBloc, like other decentralized contact tracking programs. Value Focused Thinking (VFT) is used to examine the effectiveness of blockchain-based decentralized apps in crowd management and contact tracking for the Tokyo Olympics. A VFT structure helps to reduce the number of fundamental and strategic goals that need to be considered for effective contact tracing and crowd control by taking stakeholder viewpoints into account. In [48], the authors have made a comparison between the goals specified by VFT and the characteristics of blockchain technology.

2.2.2 Connect:

The virus's spread appears to be too quick for laborious and ineffectual human contact tracking measures to halt it. "Connect", a blockchain-enabled digital contact tracking system that may use information on verified samples and alert people in their close vicinity, was developed by the authors to solve this problem and slow the rate at which the virus spreads [13]. If many individuals used the platform and profited from the targeted ideas, this would be very beneficial.

2.2.3 Blockchain-Driven Contact Tracing System (BDCT) and P2B-Trace:

The majority of current approaches appear to be elevated designs with little opposition, and they view blockchain as just a completely separate storage solution that aids third-party central data centers, ignoring the importance and potential of the consensus protocol and incentive mechanism [32]. Few writers offered a simple, free Blockchain-Driven Contact Tracing system (BDCT) to close the gap. The BDCT framework suggests an RSA encryption-based transaction verification method (RSA-TVM) to guarantee contact tracing correctness. This method has achieved more than 96 percent contact instance trying to record accuracy even though each person has a 60% chance of failing to verify the contact details [40]. Additionally suggested is P2B-Trace, a blockchain-based project for contact tracking that protects user privacy [45]. In order to prevent data modification, a decentralized architecture is meant to capture the ADS of contact record maintenance. The authors then suggested a zero-knowledge presence categorization algorithm as a way to validate proximity claims while maintaining privacy.

2.2.4 BeepTrace:

With the aim of decreasing the epidemic and resolving privacy concerns associated with contact tracking, unique contact tracing mobile software called "BeepTrace" was created by authors of [31]. The software has two modes: passive and active. Passive mode uses GPS to locate contacts; active mode uses Bluetooth Low Energy (BLE) technology. Based on the communications network they employ, contact tracing techniques might be categorized as follows: BLE is largely used by location-based solutions, whereas RFID is mostly used by proximity-based solutions [47].

2.2.5 BlueTrace:

An application protocol called "BlueTrace" enables people to track their online relationships in an effort to stop the COVID-19 epidemic from spreading [15] . The Singaporean government's BlueTrace authorized the contact tracing once again for the TraceTogether app. The authors of [56] proposed a low-fidelity virtual computer prototype that aids in the transmission of infections through interactions with humans at points of contact throughout time, particularly the transmitting graph structure. Using this disease dissemination model, we could then compare outbreak trajectories with or without peer-to-peer contact tracking.

2.2.6 Automated and Manual Contact Tracing:

The authors of [24] have presented a decentralized blockchain-based contact tracing solution and shown how blockchain-based immutable records might in fact enhance the trustworthiness, transparency, and accountability of COVID-19 contact tracking programs. In their study, they have protected user data through contact tracing solutions by utilizing built-in blockchain characteristics. User's privacy is protected by their suggested solution since it gives them the option to decide how and with whom their data will be shared. More distant users approaches are anticipated to be utilized for the purpose of contact tracing and appear to be on the market as a result of the development of 5G- and beyond-5G-positioning research, according to [49].

Automated contact tracing applications can offer quick and accurate tracing services compared to the more expensive human tracing method; nevertheless, excessive efficiency may cause privacy problems for app users. In an automated tracing situation, an efficient confidentiality solution is developed using the beneficial properties of blockchain [27]. One common technique combines multi-signature with public key clustering, non-interactive zero-knowledge evidence, or both. The work

of recognizing connections by many alternative signatures from various contacts at the collaborative engagement stage can be completed with zero knowledge verified proof [35, 51].

However, even on a large scale, manual contact tracing is likely to be required in most cases, and additional study is unquestionably required to strengthen the scientific foundation for autonomous vehicle contact tracing [18]. Future research should evaluate the effects of infection transmission based on the available evidence, as well as the technical aspects of contact-tracing apps (efficiency and absorption), as well as the application interactions with manual contact-tracing systems and the ethical and equitable considerations that they raise [9].

The existing contact tracking method has three shortcomings. User's very sensitive personal information may be revealed to a third party or organization and it is held in a central database that might be accused of theft and tampering with [52]. The effectiveness of established contact tracing procedures is highly constrained since they primarily focus on data exchange through a single dimension, such as location-based tracing. It is essential to create a blockchain-based digital contact tracing method that delivers contact tracing effectively without endangering the privacy or confidentiality of users [26]. People may withdraw their information at any time using blockchain, which gives them full access to it at all times during its existence [25].

3 CTChain: Platform Design

Our suggested design uses blockchain technology and a well defined network hierarchy to gather and handle connections between users for contact tracing. User identification, region mempool, region handler, and result analytics make up its four main building blocks. These blocks are connected to a number of other entities, such as the city node, hospital node, event verification, region risk calculation, blockchain processing, and broadcasting results.

3.1 CTChain Architecture Overview

The proposed CTChain structure makes use of specialized nodes to meet the demanding requirements of the *hospital, city, and user activities* as shown in Figure 1. From the user's localized chains, the hospital node constructs and bundles them to be delivered to the city-level nodes. Once the users 'at-risk' have been located, the mobile client transmits a transaction block to the hospital node as shown in (Table 1). The user's personal ID and the time of contact are hashed information in this block, which is necessary to build the ultimate city/regional blockchain. The information about the infection is given to the *region handler* through the mempool after being first checked for data validity by the second-level city node. The infection will be added to the region-specific cache *only if* it is pertinent in terms of risk level or time of encounter. Otherwise, it will be eliminated as a past-due event. The map shown in Figure 1 is divided into specific zones based on risk statistics (low, medium and high) to illustrate the gradations of severely infectious to safe regions.

3.2 Client Node

The mobile client that collects user information and transmits transactions between users makes up the user identification block. The procedure begins with the gathering of user data, which is then packaged into transactions or events. The client then sends this data to a hospital node using infection or recovery values that have been established. People's user-Ids, geolocation, timestamps, and a flag indicating whether or not they are infected with COVID are all collected by our system. Additionally, since Bluetooth is used to identify and communicate a user's position, anonymization can only occur when an ID is provided to the user in place of a name or other identifier. Data that enters the network is first transmitted to the client node for ultimate archival and processing. When new clients want to join the network, the client node serves as the network manager. The user handshakes with the client node at a known IP address after becoming a member of the network and seeks a parent node by submitting their current information (location mainly).

The user's whole profile, including name, user ID, demographic data, and history of interaction with the pathogen, is kept in a separate block. In order to re-verify the transactions, update the block, and the mempool, the acquired data is updated every five minutes. Multiple mini-mempools that are specific to each newly constructed area are produced once the transactions have been updated in the region mempool. After this, it will continue to add blocks to the chain. Each block in a blockchain is given a distinct nonce and hash, but it also refers to the hash of a previous block in the chain, which makes mining blocks challenging, especially on big networks.

3.3 Hospital Node

A key component of our design is the hospital node, which enables medical personnel to immediately acquire infection information for an area and send infection alarms to the network while also dividing the responsibility of the nodes into smaller entities. These hospital nodes learn about a client and their shared certificates, and they use that information to approve incoming transactions from a particular client. Through an infection occurrence or transaction, it can also get direct infection information. If the hospital node traces out a certain individual as infected during a given time period, it will result in a change in the user's status and return all prospective users who are also at risk. Additionally, the parent city-level node can provide risk region changes to the hospital node. The existing list of risky or dangerous zones are simply updated by this new infection information.

Every block that the hospital node adds to its blockchain is copied and sent to another node. These blocks include a list of events that the city node subsequently unpacks, analyzes, and prepares a chain to upload the data for the city-level regional infection map. This saves memory by providing the

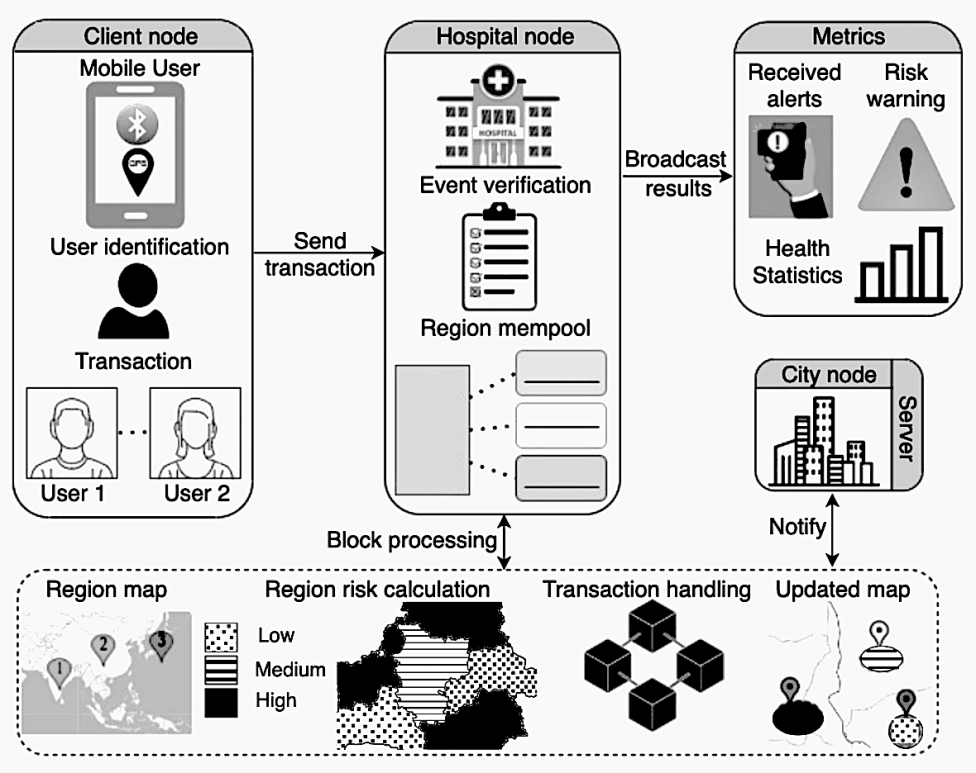


Figure 1: This is our hierarchical architecture for contact tracing. This framework consists of client node, hospital node, local mempool, region handler, city node and result broadcast

city node with its own region handler. It takes the current legitimate "events" that include information that complies with the requirements of python dictionaries. These occurrences are recorded in a list known as a "block" which is added to the collection of blocks that makes up the blockchain and is signed to be processed further. The hospital node just verifies that each event contains the necessary keys and values for the purposes for which it is required. For instance, a location event requires current location coordinates, while a new illness event requires the infection state. On the blockchain, verification also takes place, although this largely only entails making sure that all hashes and blocks are congruent.

The information about the cities is contrasted with a select group of currently severely affected areas. The user immediately receives a notification to switch to location mode and is informed of any possible risks if the location is in a highly contagious area. The user receives a notice that the data has been "recovered" after it has been placed in the mempool. The extra data is accounted for, verified, and built into a new block using hashlib (which offers a unified interface to all the secured hash), which is then processed through the merkle hash, verified against the rest of the blockchain, and added to the blockchain created when the mempool or cache reaches its capacity (the minimum block size of 100 in testing). The city node then receives a copy of this filled block that will be used for generating health advisories.

3.4 Region Handler

Any node that monitors specific 'regions' in an area is operated by the Region Handler module. As shown in Figure 2 it verifies the transactions as the gathered events are provided to this node to make sure whether the user is in its region-of-interest. If they are, the region handler adds their event to a temporary list of events associated to that particular region to check its risk, and then sends the results back to the node, passing the warning to the user. Any node can query the region handler for statistics such the percent people infected per unit area per hour (PPH). The health administrators are responsible for identifying regions based on the geography of the area since the region handler can add/remove regions at the request of its node.

The areas are classified into three groups based on the infection rate in Figure 1. The area highlighted in black is deemed to be at high risk of infection if the infection rate is more than 50%. Similarly, the region with dot pattern has a low infection rate with less than 20% of the people affected, while the region with line pattern has a moderate infection rate between 20 and 50 percent. The major goal is to situate the regions in locations with more human activity, such as malls, companies, or restaurants. Each region is manually specified by an administrator. Every time the node receives a request to add a new region, it sends the region's name and coordinates to the region handler, which adds the new region to its list of managed

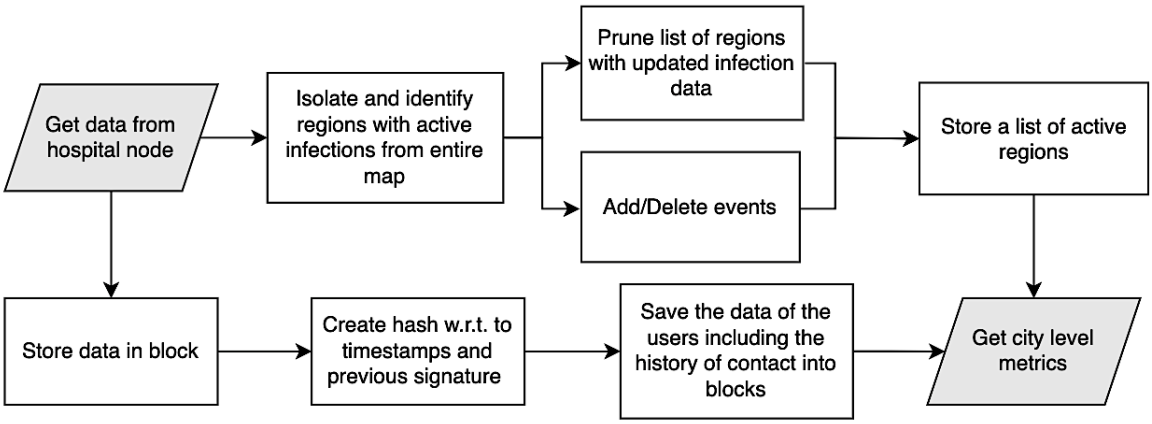


Figure 2: Processing through region handler in blockchain

Table 1: Sample block data

Sample Block Data	
Name of Entities	**Sample Data**
Index number of block	001032
Current Block Signature (32-byte)	ahK4CTbkjwbxg6HVH...
Previous Block Signature (32-byte)	oBHBuns3nxsyim4k...
Public key of creator (64-byte)	MMGvigqkagd9d8...
Creator Name of the block	Heart 'Medical Center'
ID of creator	VMAC007
Node type of creator	'Client node'
Timestamp of creator	84432214770.69
IP of creator node	127.0.0.1:295
Block events at city node	
Node Id	I-0010046828592
Type of event	"Contact Event"
User ID's	*userA*: "O-001...", *userB*: "O-002..."
Status of user	*statusA*: "At-Risk", *statusB*: "Infected"

regions and, if required, extends the "primary region box" to incorporate it. The map is updated and the areas are defined in this way.

The region handler stores each region as a separate python dictionary. Each one of them includes the region's name and latitude and longitude coordinates. Additionally, a list for recent events is given to each area. For testing purposes, additional lists are also provided for metric data storage; however, in the final product, the metrics would likely be handled by a distinct entity. The information about an incoming event is added to the region's list of recent events if it occurs inside that region. The region handler will delete any obsolete transactions from each area after the processing is finished (such as determining PPH or the percentage of infected files where in our case this is any transaction over 1 day old).The whole list of all the regions is kept in a JSON file and may be reloaded, deleted, or both (still keeping the collection of regions, just without recent events).

3.5 City Node

The city node serves as the primary data processor, where we establish the areas and carry out computations based on those regions. These nodes have the ability to transmit a group of "high risk users" and "high risk locations" to their child hospital nodes (this is done as a response to the hospital node sending up a block). The city node transmits the necessary metrics to the client and the hospital node by relying on the data that is processed from the region handler. The city node processes all "transactions" by passing them via the Region Handler, which explicitly examines the "transaction location" using the regions set up on the global map.

The city node determines the precise region where the "transaction" is recorded by checking each established region one at a time. If the "transaction" is possibly in a specified region, we add that transaction to the region's current "mempool" and delete any existing old data (a period of 1 day). In order to estimate the risk calculation measure, we later compute the population density and the proportion of affected people. If a transaction is not in a designated region, it is placed in the "mempool" and handled on a much bigger scale in the same manner as the hospital node. These areas can provide a list of non-infected ("at risk") travelers who have visited there. The city node may take transactions originating from new areas and provide risk estimations for all regions, just like hospital nodes, which can also accept transactions related to infection. The blocks passed or registered by the child hospital nodes provide the transaction information to these city nodes. Following the unpacking of these blocks, the city node's mempool cache are used to hold all of the transactions. The hospital node and the users at the client level are also recipients of the city node's

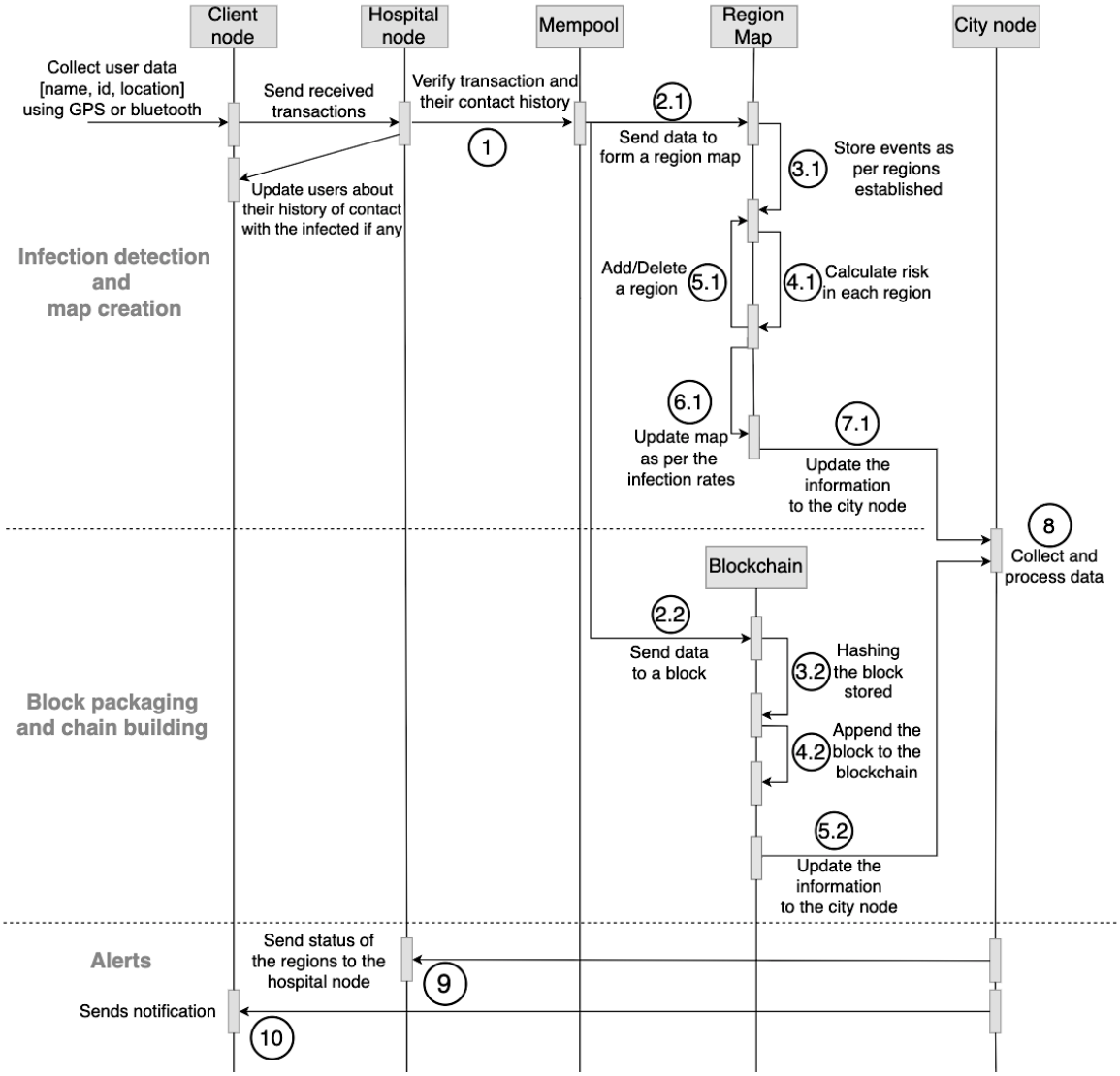


Figure 3: This is the sequence diagram for our hierarchical framework. The core process happens at the blue blocks in the processing detection level. It has 15 steps that shows how the data is carried out to the framework and back to the client

results.

3.6 CTChain Sequence

The framework's sequence diagram is shown in Figure 3. At the beginning, client node gathers user information and transmits the transaction to the hospital node. Verification of transactions, contact history checks, and storage in the mempool comes into action. The infection detection and map-creation level, which is the initial component of the architecture helps in performing the actions on the established map, where it stores events, calculates the risk of a region and updates the map. This aids in drawing the boundaries of a territory on the existing map and the event is recorded in a blockchain. The data is hashed and then used to estimate risk in various places, updating the map of those regions in line with the most recent infection rates and this process takes place in the block packaging and chain building level. In every cycle, the danger is continually computed, allowing the map's areas to be added or removed depending on the rate of infection. The new information entered into the blockchain and the updated region map data is forwarded to the city node where it informs the hospital node of the condition of various regions and sends messages or alerts to the client node's users.

3.6.1 Advisory and Alert Handling:

A city official can track the spread of an infection within a given area (a hospital, a city, or an entire region) and base decisions on this information. For example, the official might pass ordinances requiring people to wear masks or to stay at

Algorithm 1 Client level transaction workflow

```
Client: C
Transaction: t
Region handler: R
Region specific risk of infection: r
Mempool Cache: cache
Begin
while Incoming 't' == true: do
    Validate and verify 't'
    if 't' is valid: then
        Verify identity of C
        Send verified 't' to cache
        Send 't' to R
        if 't' falls in valid region: then
            Alert 'C' about current r
            Request 'C' to shift to send GPS data
            Backtrack every 5 minutes to get recent contacts
        else
            if 't' is not in valid region: then
                Request 'C' to send Bluetooth data
                Repeat the process from line 7
    while 't' is stored: do
        Add 't' to region-specific cache
        Clean outdated 't'
        Retrieve r
        Alert 'C' about the region's r
if cache is full: then
    Package all t in cache into a block
    Append block to the blockchain
    Push block up to parent City node
    Clear the cache
End
```

home, depending on how widely the infection gets spread and how many people are getting ill. They can also make a decision to isolate a certain area based on regional considerations (like a mall that has high infection risk). The program now only notifies users of potential risks based on their most recent interaction history. For example, if an individual comes in contact with a sick person, or enter a high-risk region, he/she will receive alerts accordingly.

4 Evaluation Results

4.1 Tools and Platform

This project uses several tools to construct CTChain application, and perform simulation for user movement through the regions. Before writing the software, we looked for a realistic simulator to give us user data that we could run with the software. For this simulation, we are using an open-source GitHub project called "trip-simulator" made by SharedStreets[36]. This trip simulator is ran through NPM, and constructs a JSON file of vehicles (users), and the paths

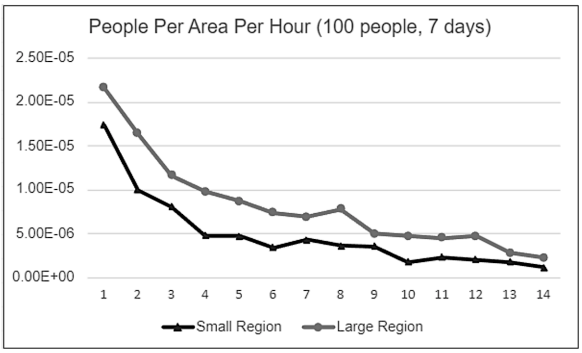


Figure 4: PPH for 100 people

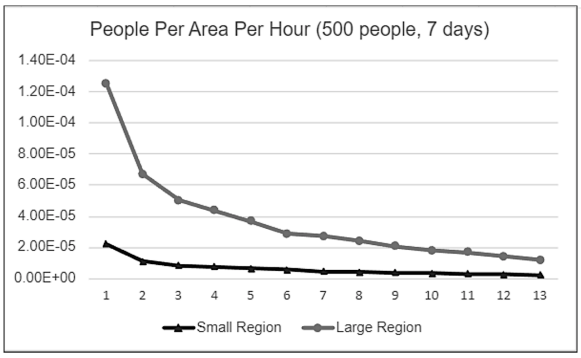


Figure 5: PPH for 500 people

that they have travelled over a given period of time. These simulations were ran for groups of 100, 200, and 500 users; and the simulated times included 1 day, 7 days, 14 days, 21 days, and 28 days. With the output JSON files, we ran a Python script to remove excess identifier data, and converted the collection of paths into a collection of points and timestamps.

Our software is written in Python 3.0 and uses several libraries for additional functionalities. These libraries include the following: 'flask' allows nodes to host their own servers and receive requests using the HTTPS protocol. These 'requests' allow both clients and nodes to send the different types of data (transactions, blocks, and statistics) back and forth. We also used 'pycryptodome' and 'ssl' for certificates and cryptographic hashing to make sure that all data being sent over the network is secure and verifiable. Python libraries 'pandas' and 'numpy' are used together to process large data sets and give us easy-to work with results data. Aside from these software tools, we also made use of the Microsoft suite, mainly Excel, to view and graph our collected results. Running simulations took between 15 minutes to a few hours depending on the average size of the incoming data. These simulations were ran on a AMD CPU with 16 GB of RAM.

4.2 Result Discussion

We are evaluating CTChain capability to map out the active infections in terms of three different parameters: sparse vs

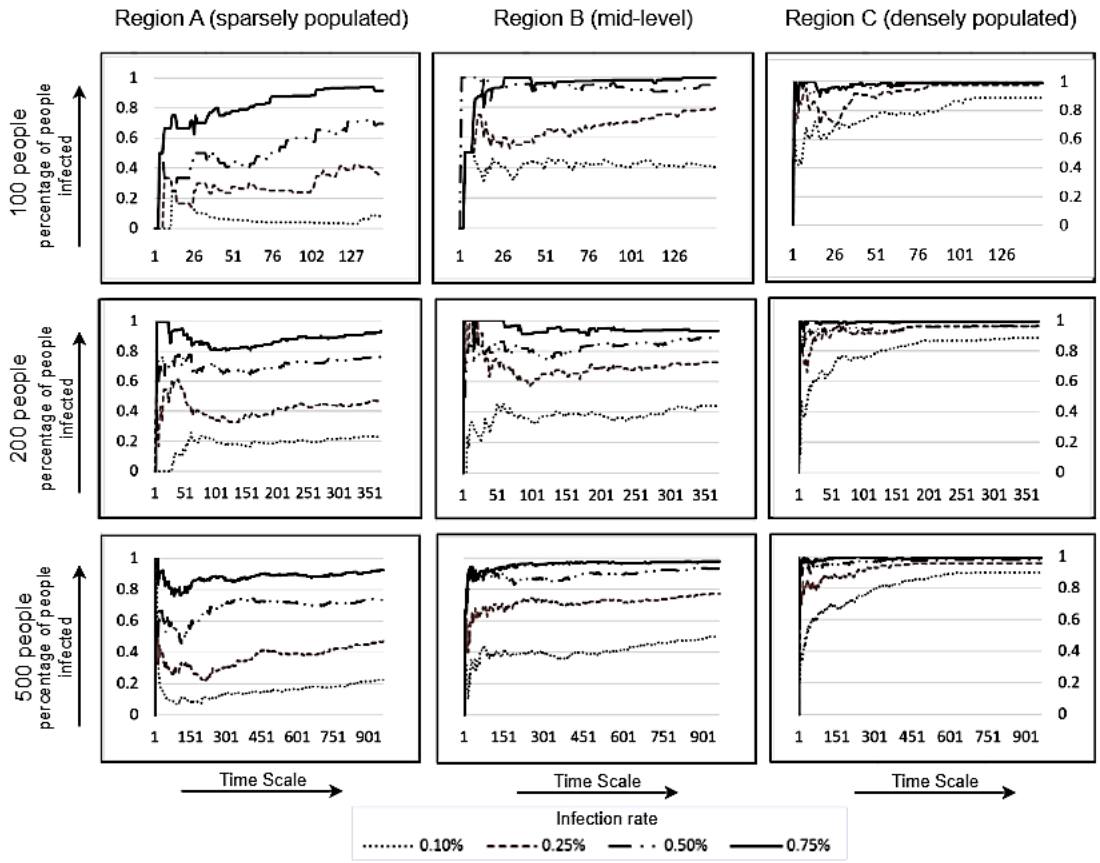


Figure 6: Result graphs

densely populated region, number of people in each region, and initial infection rate. Our goal is to show concrete efficacy results that our platform can scale well through various cases of mild to seriously infectious. To begin, we devised a new metric termed as PPH to determine activity level of specific regions.

PPH itself stands for "people per area per hour." For each region, this metric is calculated by taking the list of events from a regions mempool over the course of the most recent hour, and dividing this number by the area of the region (in square degrees latitude/longitude). The proper formula for this is as follows:$(\textit{number of events in the last hour})/(\textit{degree latitude} * \textit{degree longitude})$.

The results for the number of active people in each region during a certain period of time are shown in Figures 4 and 5. These graphs visually represent that the densely populated region receives approximately twice the foot-traffic as compared to the sparse one. These visuals are independent of any infection data and present a minimalist view of each region just with the increase in the ongoing traffic.

We have constructed a 3×3 grid in Figure 6 to show the variations of the percentage of population infected w.r.t. independent parameters such as total people passing through the region, population density, initial infection rate, and time. The goal of this grid-view is to depict that the *platform can handle transactions a wide variation from mild to complex infection rates cases in sparsely or densely populated regions*. The first column (leftmost) represents the low population density Region A, whereas the rightmost column is the most popular Region C and Region B is moderately populated. This experiment has been carried out with 100, 200, and 500 people per region which is represented as each row. Within each subplot, the x-axis represents the time scale and the y-axis shows the percentage of people infected w.r.t. entire regional population. Each graph further has four different characteristics to represent initial infection rates ranging from 10% to 75%. For example, in the lowest data point only 1 out of 10 people are COVID-19 positive initially. The rest of x-axis shows the progression of infection through the regional population.

It is evident from each and every graph in Figure 6 that as the initial rates increase, the number of infection cases also increases as expected. We begin the deep-dive by investigating the *first row* of 100 people in the various regions. It is observed that the steady-state values becomes higher from sparse to densely populated areas (left to right), even with low initial infection rate. Moreover, things deteriorate at a faster pace in Region C as compared to Region A. Thus, the population density is the deterministic factor for the probability of contracting infection in comparison to the other

initial conditions. This verifies the merits of social distancing directives from Center for Disease Control (CDC) and real-life phenomena where people were migrating away from the cities to escape from the peak of the pandemic.

We next explore the *column-wise* 3×3 grid, beginning with the lowest population density of Region A (1^{st} column). It is observed that the processing time increases with the change in the x-axis scale for the exact same 7-day period. Although the infection trends remain mostly consistent for each region as the population grows, CTChain scales accordingly to accommodate the increased transactions. Our framework limits the number of incoming requests from the client to the hospital node, preventing the server congestion at the higher levels. The most remarkable results are in Region C (last column) when almost the entire population gets infected and thereby will need substantial medical help from the administrators. We are presenting week long data in Figure 6, but the patterns continue to remain consistent for month long simulation as well. Hence, we are skipping them for brevity.

5 Conclusion

The healthcare system across the entire world has been over-stretched beyond limits to address the extremely precarious aftermaths of the Covid-19 pandemic for the past few years. Non-Pharmaceutical Intervention in form of contact tracing for infection containment can be laborious, adhoc and a time-consuming process. Although digital solutions are emerging in the wake of the pandemic, concrete design details especially for linking user information with active infection regional maps are lacking. Our CTChain uses blockchain-based hierarchical node structure to improve the performance and efficacy of this process. The chain model stores transactions in an anonymized and immutable way, allowing for accurate data as well as publicly available statistics. The blockchains work by allowing quick and consistent access to blocks of information, that can be processed for risk calculations, user infection alerts, region/global statistics, and much more.

Through the use of specially designed region handler, we are able to see the infection spread and region "popularity" (PPH) at a per-region level. This allows even faster response times for users entering specific regions, as well as providing metrics that can be used in the future to determine trends in how infections will spread throughout given regions. We show concrete results that our platform can handle wide variation of infection ranging from mild to highly contagious regions. This allows for more specified mandates, such as temporarily shutting down certain unacceptably risky regions, to mitigate the number of users getting sick. Our model is better than state-of-art design as it works on a hierarchical and is more publicly accessible. It is efficient for larger complex systems as it can be scaled on a wider level. Moreover, it has reduced vulnerability to a single point of failure as multiple copies of the chain stored throughout the network. PoA makes it more trustworthy with open public architecture and thus relevant for multi-modal data storage and sorting for contact tracing. In the future, we want to use smart contracts to offload intelligent processing data and issue automated notifications in a refined manner.

Acknowledgments

We are grateful to Southeast Missouri State University's Grants and Research Funding Committee (GRFC) and Computer Science Dept for funding our project.

References

[1] "COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University", https://coronavirus.jhu.edu/map.html, May, 2022.

[2] "NHS COVID-19. A Voluntary Contact Tracing App for Monitoring the Spread of the COVID-19 Pandemic in England and Wales", https://covid19.nhs.uk/, NHS COVID-19 App Support, August 2020.

[3] "Transmission of SARS-CoV-2:Implications for Infection Prevention Precautions. SARS-CoV-2 is a member of a Large Family of Viruses called Coronaviruses. These Viruses can Infect People and Some Animals", World Health Organization, July 2020.

[4] "CDC COVID Data Tracker, CDC Recommends use of COVID-19 Community Levels to Determine the Impact of COVID-19 on Communities and to Take Action", Centers for Disease Control and Prevention, US Department of Health and Human Services, CDC, Mar 2022.

[5] "COVID Alert NY" is a Voluntary, Anonymous, Exposure-Notification Smartphone App. The App is Programmed to Collect Information on Exposures to Covid-19-Positive Individuals within Six Feet for Longer Than 10 Minutes, NY Department of Health, Mar 2022.

[6] "COVIDWISE is Virginia's Official Exposure Notifications App that Lets you Know if You've Likely been Exposed to another COVIDWISE User with a Verified Positive Covid-19 Test Result", Virginia Department of Health, Mar 2022.

[7] WHO Covid-19 Dashboard, The World Health Organization is a Specialized Agency of the United Nations Responsible for International Public Health. The WHO Constitution States its Main Objective as "The Attainment by all People of the Highest Possible Level of Health"., Mar 2022.

[8] Roba Abbas and Katina Michael. "COVID-19 Contact Trace App Deployments: Learnings from Australia and Singapore". *IEEE Consumer Electronics Magazine*, 9(5):65–70, 2020.

[9] Julia Amann, Joanna Sleigh, and Effy Vayena. "Digital Contact-Tracing during the Covid-19 Pandemic: An Analysis of Newspaper Coverage in Germany, Austria, and Switzerland". *Plos one*, 16(2):e0246524, 2021.

[10] Md Murshedul Arifeen, Abdullah Al Mamun, M Shamim Kaiser, and Mufti Mahmud. "Blockchain-Enable Contact Tracing for Preserving User Privacy during COVID-19 Outbreak", 2020.

[11] Gennaro Avitabile, Vincenzo Botta, Vincenzo Iovino, and Ivan Visconti. "Towards Defeating Mass Surveillance and SARS-Cov-2: The Pronto-c2 fully Decentralized Automatic Contact Tracing System". *Cryptology ePrint Archive*, 2020.

[12] Michael G Baker, Nick Wilson, and Andrew Anglemyer. "Successful Elimination of Covid-19 Transmission in New Zealand". *New England Journal of Medicine*, 383(8):e56, 2020.

[13] Eranga Bandara, Xueping Liang, Peter Foytik, Sachin Shetty, Crissie Hall, Daniel Bowden, Nalin Ranasinghe, and Kasun De Zoysa. "A Blockchain Empowered and Privacy Preserving Digital Contact Tracing Platform". *Information Processing & Management*, 58(4):102572, 2021.

[14] Lars Baumgärtner, Alexandra Dmitrienko, Bernd Freisleben, Alexander Gruler, Jonas Höchst, Joshua Kühlberg, Mira Mezini, Richard Mitev, Markus Miettinen, Anel Muhamedagic, et al. "Mind the Gap:" Security & Privacy Risks of Contact Tracing Apps. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, pp. 458-467, 2020.

[15] Jason Bay, Joel Kek, Alvin Tan, Chai Sheng Hau, Lai Yongquan, Janice Tan, and Tang Anh Quy. "BlueTrace:" A Privacy-Preserving Protocol for Community-Driven Contact Tracing Across Borders. *Government Technology Agency-Singapore, Tech. Rep*, 18, 2020.

[16] Yoshua Bengio, Richard Janda, Yun William Yu, Daphne Ippolito, Max Jarvie, Dan Pilat, Brooke Struck, Sekoul Krastev, and Abhinav Sharma. "The Need for Privacy with Public Digital Contact Tracing during the COVID-19 Pandemic". *The Lancet Digital Health*, 2(7):e342–e344, 2020.

[17] Wasilij Beskorovajnov, Felix Dörre, Gunnar Hartung, Alexander Koch, Jörn Müller-Quade, and Thorsten Strufe. "Contra Corona: Contact Tracing against the Coronavirus by Bridging the Centralized-Decentralized Divide for Stronger Privacy". In *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, pp. 665-695, 2021.

[18] Isobel Braithwaite, Thomas Callender, Miriam Bullock, and Robert W Aldridge. "Automated and Partly Automated Contact Tracing: A Systematic Review to Inform the Control of COVID-19". *The Lancet Digital Health*, 2(11):e607–e621, 2020.

[19] Louis Yat Hin Chan, Baoyin Yuan, and Matteo Convertino. "COVID-19 Non-Pharmaceutical Intervention Portfolio Effectiveness and Risk Communication Predominance", Nature Publishing Group. *Scientific Reports*, 11(1):1–17, 2021.

[20] Giuseppe Ciaburro. "blockchain Technology for Contact Tracing During COVID-19". In *Transformations Through Blockchain Technology*. Springer, pp. 201-229, 2022.

[21] Benjamin J Cowling, Sheikh Taslim Ali, Tiffany WY Ng, Tim K Tsang, Julian CM Li, Min Whui Fong, Qiuyan Liao, Mike YW Kwan, So Lun Lee, and Susan S Chiu. "Impact Assessment of Non-Pharmaceutical Interventions against Coronavirus Disease 2020 and Influenza in Hong Kong: an Observational Study". *The Lancet. Public health*, 5(5):e279–e288, 2020.

[22] Darren Flynn, Eoin Moloney, Nawaraj Bhattarai, Jason Scott, Matthew Breckons, Leah Avery, and Naomi Moy. "COVID-19 Pandemic in the United Kingdom". *Health Policy and Technology*, 9(4):673–691, 2020.

[23] Muhammad Hamza, Arif Ali Khan, and Muhammad Azeem Akbar. "Towards a Secure Global Contact Tracing App for Covid-19". In *The International Conference on Evaluation and Assessment in Software Engineering 2022*, pp. 453-460, 2022.

[24] Haya R Hasan, Khaled Salah, Raja Jayaraman, Ibrar Yaqoob, Mohammed Omar, and Samer Ellahham. Covid-19 contact tracing using blockchain. *Ieee Access*, 9:62956–62971, 2021.

[25] Robert Hinch, Will Probert, Anel Nurtay, Michelle Kendall, Chris Wymant, Matthew Hall, Katrina Lythgoe, Ana Bulas Cruz, Lele Zhao, Andrea Stewart, et al. "Effective Configurations of a Digital Contact Tracing App: A Report to NHSX". *Retrieved July*, 23:2020, 2020.

[26] Sheikh Mohammad Idrees, Mariusz Nowostawski, and Roshan Jameel. "Blockchain-Based Digital Contact Tracing Apps for COVID-19 Pandemic Management: Issues, Challenges, Solutions, and Future Directions", JMIR Publications Inc., Toronto, Canada. *JMIR Medical Informatics*, 9(2):e25245, 2021.

[27] Oritsebawo Paul Ikpobe and John Easton. "Can Blockchain Take Smartphones Out of Contact Tracing?". *The Journal of The British Blockchain Association*, p. 30993, 2021.

[28] Rawan Jalabneh, Haniya Zehra Syed, Sunitha Pillai, Ehsanul Hoque Apu, Molla Rashied Hussein, Russell Kabir, SM Arafat, Md Majumder, Anwarul Azim, and Shailendra K Saxena. "Use of Mobile Phone Apps For Contact Tracing to Control the COVID-19 Pandemic: A Literature Review". *Applications of Artificial Intelligence in COVID-19*, pp. 389 - 404, 2021.

[29] Ashok Jhunjhunwala. "Role of Telecom Network to Manage COVID-19 in India: Aarogya Setu". *Transactions of the Indian National Academy of Engineering*, 5(2):157–161, 2020.

[30] Jill Juergensen, José Guimón, and Rajneesh Narula. "European SMES Amidst the COVID-19 Crisis: Assessing Impact and Policy Responses". *Journal of Industrial and Business Economics*, 47(3):499–510, 2020.

[31] Hong Kang, Zaixin Zhang, Junyi Dong, Yinghao Ji, Hao Xu, and Lei Zhang. Beeptrace for covid-19 pandemic: A demo. In *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pages 1–2. IEEE, 2021.

[32] Anjum Khurshid et al. "Applying Blockchain Technology to Address the Crisis of Trust During the COVID-19 Pandemic". *JMIR Medical Informatics*, 8(9):e20477, 2020.

[33] Franck Legendre, Mathias Humbert, Alain Mermoud, and Vincent Lenders. "Contact Tracing: An Overview of Technologies and Cyber Risks". *arXiv preprint arXiv:2007.02806*, 2020.

[34] Jinfeng Li and Xinyi Guo. "COVID-19 Contact-Tracing Apps: A Survey on the Global Deployment and Challenges". *arXiv preprint arXiv:2005.03599*, 2020.

[35] Momeng Liu, Zeyu Zhang, Wenqiang Chai, and Baocang Wang. "Privacy-Preserving COVID-19 Contact Tracing Solution based on Blockchain". *Computer Standards & Interfaces*, 83:103643, 2023.

[36] Robin Lovelace. "Open Source Tools for Geographic Analysis in Transport Planning". *Journal of Geographical Systems*, 23(4):547–578, 2021.

[37] Carolina Lucas. "Longitudinal Analyses Reveal Immunological Misfiring in Severe COVID-19". *Nature*, 584(7821):463–469, 2020.

[38] Wenzhe Lv, Sheng Wu, Chunxiao Jiang, Yuanhao Cui, Xuesong Qiu, and Yan Zhang. "Decentralized Blockchain for Privacy-Preserving Large-Scale Contact Tracing". *arXiv preprint arXiv:2007.00894*, 2020.

[39] Leonardo Maccari and Valeria Cagno. "Do We Need A Contact Tracing App?". *Computer Communications*, 166:9–18, 2021.

[40] Dounia Marbouh, Tayaba Abbasi, Fatema Maasmi, Ilhaam A Omar, Mazin S Debe, Khaled Salah, Raja Jayaraman, and Samer Ellahham. "Blockchain for COVID-19: Review, Opportunities, and A Trusted Tracking System". *Arabian Journal for Science and Engineering*, 45(12):9895–9911, 2020.

[41] James O'Connell, Manzar Abbas, Sarah Beecham, Jim Buckley, Muslim Chochlov, Brian Fitzgerald, Liam Glynn, Kevin Johnson, John Laffey, Bairbre McNicholas, et al. "Best Practice Guidance For Digital Contact Tracing Apps: A Cross-Disciplinary Review of the Literature". *JMIR mHealth and uHealth*, 9(6):e27753, 2021.

[42] Deepraj Pandey, Nandini Agrawal, and Mahabir Prasad Jhanwar. "CovidBloc: A Blockchain Powered Exposure Database for Contact Tracing". *Cryptology ePrint Archive*, 2020.

[43] Anupam Pattanayak, Subhasish Dhal, and Sourav Kanti Addya. "Automatic Privacy-Preserving Contact Tracing of Novel Coronavirus Infection by Cloud-Enabled WBAN using Blockchain". *Cryptology ePrint Archive*, 2020.

[44] Jason L Payne and Natalia Hanley. "COVID-19 and Corrections in Australia: A Summary Review of the Available Data and Literature". *Victims & Offenders*, 15(7-8):1367–1384, 2020.

[45] Zhe Peng, Cheng Xu, Haixin Wang, Jinbin Huang, Jianliang Xu, and Xiaowen Chu. "P2b-Trace: Privacy-Preserving Blockchain-based Contact Tracing to Combat Pandemics". In *Proceedings of the 2021 International Conference on Management of Data*, pp. 2389-2393, 2021.

[46] Moritz Platt, Anton Hasselgren, Juan Manuel Román-Belmonte, Marcela Tuler De Oliveira, Hortensia De la Corte-Rodríguez, Sílvia Delgado Olabarriaga, E Carlos Rodríguez-Merchán, Tim Ken Mackey, et al. "Test, Trace, and put on the Blockchain?: A Viewpoint Evaluating the Use of Decentralized Systems for Algorithmic Cntact Tracing to Combat a Global Pandemic". *JMIR Public Health and Surveillance*, 7(4):e26460, 2021.

[47] Laura Ricci, Damiano Di Francesco Maesa, Alfredo Favenza, and Enrico Ferro. "Blockchains for Covid-19 Contact Tracing and Vaccine Support: A Systematic Review". *Ieee Access*, 9:37936–37950, 2021.

[48] Rishi Sabarigirisan, Aditi Biswas, Ridhi Rohatgi, KC Shyam, and Shekhar Shukla. "Leveraging Blockchain Based Decentralized Apps for the Tokyo Olympics Amid the COVID-19 Pandemic". *First Monday*, 2021.

[49] Viktoriia Shubina, Sylvia Holcer, Michael Gould, and Elena Simona Lohan. "Survey of Decentralized Solutions with Mobile Devices for User Location Tracking,

Poximity Detection, and Contact Tracing in the Covid-19 Era". *Data*, 5(4):87, 2020.

[50] Viktoriia Shubina, Aleksandr Ometov, and Elena Simona Lohan. "Technical Perspectives of Contact-Tracing Applications on Wearables for COVID-19 Control". In *2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pages 229–235. IEEE, 2020.

[51] Lucy Simko, Ryan Calo, Franziska Roesner, and Tadayoshi Kohno. "COVID-19 Contact Tracing and Privacy: Studying Opinion and Preferences". *arXiv preprint arXiv:2005.06056*, 2020.

[52] Jinyue Song, Tianbo Gu, Zheng Fang, Xiaotao Feng, Yunjie Ge, Hao Fu, Pengfei Hu, and Prasant Mohapatra. "Blockchain Meets COVID-19: A Framework for Contact Information Sharing and Risk Notification System". In *2021 IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*. IEEE, pp. 269-277, 2021.

[53] Corinne N Thompson, Jennifer Baumgartner, Carolina Pichardo, Brian Toro, Lan Li, Robert Arciuolo, Pui Ying Chan, Judy Chen, Gretchen Culp, Alexander Davidson, et al. "COVID-19 Outbreak—New York City", February 29-June 1, 2020. *Morbidity and Mortality Weekly Report*, 69(46):1725, 2020.

[54] Serge Vaudenay. "Centralized or Decentralized? The Contact Tracing Dilemma". *Cryptology ePrint Archive*, 2020.

[55] Michel Walrave, Cato Waeterloos, and Koen Ponnet. "Adoption of a Contact Tracing App for Containing COVID-19: A Health Belief Model Approach. *JMIR Public Health and Surveillance*, 6(3):e20572, 2020.

[56] Tyler M Yasaka, Brandon M Lehrich, and Ronald Sahyouni. "Peer-to-Peer Contact Tracing: Development of a Privacy-Preserving Smartphone App". *JMIR mHealth and uHealth*, 8(4):e18936, 2020.

Blake Bleem is a senior undergraduate student in the Department of Computer Science at the Southeast Missouri State University. He is working on a bachelors in Computer Science, with a minor in Mathematics. He is the president of Competitive Programming Club, the secretary of AI Club, the vice president of Math Club. His current research interests include artificial intelligence, machine learning, blockchain.

Vishwanath Varma Indukuri is a graduate student in the Department of Computer Science at the Southeast Missouri State University. He received his bachelor's degree in Electronics and Communication engineering from Amrita Vishwa Vidyapeetham, Coimbatore, India in 2021. His current research interests include artificial intelligence, machine learning, cloud computing and blockchain.

Reshmi Mitra is an Assistant Professor in the Department of Computer Science at the Southeast Missouri State University. She received her MS and Ph.D. degrees in Electrical and Computer Engineering from the University of North Carolina at Charlotte in 2007 and 2015, respectively. Previously she has worked at the National Institute of Technology India, Advanced Micro Devices Austin, and Samsung Austin R&D Center. Her research interests include Security and Performance issues in IoT, Cloud Computing, and Blockchain.

Indranil Roy is an Assistant Professor in the Department of Computer Science at the Southeast Missouri State University. He received his MS and Ph.D. degrees in Computer Science from Southern Illinois University, Carbondale in 2018 and 2022, respectively. His current research interest includes the design of architecture and communication protocols for structured peer-to-peer overlay networks, security in overlay networks, and Blockchain.

Chaotic Map and Quadratic Residue Problems-Based Hybrid Signature Scheme

Rania Shaqbou'a* and Nedal Tahat*
The Hashemite University, Zarqa 13133, JORDAN

O. Y. Ababneh†,
Zarqa University, Zarqa, JORDAN

Obaida M. Al-Hazaimeh‡
Al-Balqa Applied University, Irbid, JORDAN

Abstract

The secure electronic signature provides contracting parties, particularly the consumer, with safety and reassurance which has a favorable impact on business transactions due to the strong legal authority supplied by this signature, which is based on a method for its formation. Therefore, researchers are rushing to design safe and performance electronic signature schemes at the same time. We offer a novel signature technique based on two hard number theory issues in this work, Quadratic Residue (QR) and Chaotic Maps (CM). Several fields of study including mathematics, physics, and computer science have taken an interest in chaotic systems as a potential tool for cryptography. Analysis demonstrates that our strategy is more secure and efficient than other connected schemes, compared to other schemes. A proof of the proposed scheme's security against known key attacks is also provided in this article.

Key Words: Chaotic maps, digital signature, quadratic residue problem, crypto-system.

1 Introduction

Secure and correct signings can only be achieved with digital signatures. Today, the traditional physical signature is outdated. Communication between colleagues in an organization is a significant issue that must be addressed securely. With a digital signature, you can send secure messages with a variety of various techniques. Information security and modern cryptography rely heavily on the use of digital signatures. It has been a long time coming, but digital signature technology is now mature and widely used in e-commerce. There are two types of digital signature algorithms based on their security presuppositions. As an example of this, consider discrete logarithm, the factorization of complex problems, or elliptic curve cryptography as methods for digital signature.

Many different techniques based on two difficult challenges have been created in order to increase the security of signature schemes: FAC and DLP [10, 16, 19]. However, several authors have also shown these schemes to be flawed [8, 9, 17]. Furthermore, there are many signature schemes based on two problems [1, 5-6, 12, 24], but these schemes need high computational complexity. As a result, the adoption of a digital signature method based on several assumptions is critical for improving system security. Based on chaotic maps and factoring issues, we have developed a digital signature algorithm. Matthews was the first to suggest a chaotic image encryption scheme [11]. There is an increasing interest in this field, and numerous approaches [3-4, 13-14, 13, 18, 27] have been presented for key-agreement protocol that is based on chaotic maps. Using a Chebyshev chaotic map's semi-group characteristic, they were able to establish the session key. Using chaotic maps and factorization issues, Chain and Kuo [5] have established an efficient and secure signature system. They were the first to use factorization issues and chaotic maps in their algorithm. But the scheme's flaw is that it necessitates a large number of keys for signature verification and signing. Using chaotic maps and factoring difficulties, we create a new signature scheme in this paper. By using an acceptable number of operations for both signature generation and verification, we demonstrate that the new scheme's performance is extremely efficient.

The remaining sections of this work are arranged as: In Section 2, we offer the requisite theory, characteristics, and notation for extended chaotic maps and factoring problems. Then in Section 3, we suggest a new signature technique. In Section 4, the suggested scheme's security and performance analysis aspects are presented. In Section 5, a numerical representation is depicted on our supplied scheme. In Section 6, we finally reach a conclusion.

2 Preliminaries

This section serves as a basic introduction to the Chebyshev chaotic map concept [2-5, 15, 18, 22, 26, 28] and the factorization problem [19] and its related mathematical properties.

* Department of Mathematics, Faculty of Science, P.O Box 330127. Email: nedal@hu.edu.jo.
† Department of Mathematics, Faculty of science.
‡ Department of Computer Science and Information Technology.

2.1 Map of Chebyshev Chaos.

The structure of the Chebyshev polynomials is reviewed in Figure 1 [20].

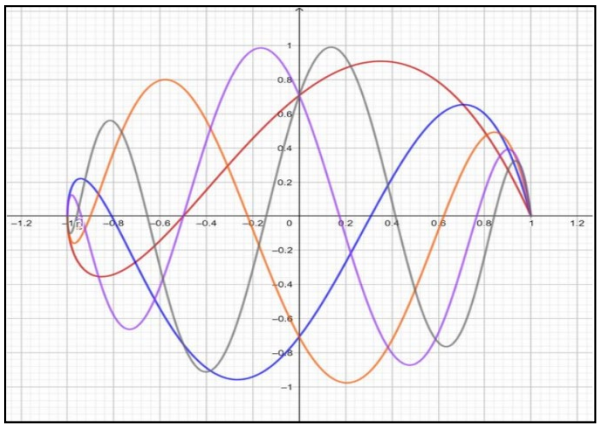


Figure 1: Chebyshev polynomials structure

A variable θ in the range [-1,1] and n is a positive integer. Let

$$T_n(\theta) : [-1,1] \longrightarrow [-1,1]$$

defined as:

$$T_n(\theta) = \cos(\theta \cos^{-1}(\theta)) \tag{1}$$

and the Chebyshev polynomial map $T_n(\theta) : \mathbb{R} \longrightarrow \mathbb{R}$ of degree n is defined by the recurrent relation

$$T_n(\theta) = 2\theta T_{n-1}(\theta) - T_{n-2}(\theta) \;;\quad n \geq 2 \tag{2}$$

where $T_0(\theta) = 1, T_1(\theta) = \theta$. Some Chebyshev polynomials are $T_2(\theta) = 2\theta^2 - 1$, $T_3(\theta) = 4\theta^3 - 3\theta, T_4(x) = 8\theta^4 - 8\theta^2 + 1$ and $T_5(\theta) = 16\theta^5 - 20\theta^3 + 5\theta$.

From (2), we get a matrix equation

$$\begin{bmatrix} T_a(\theta) \\ T_{a+1}(\theta) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 2\theta \end{bmatrix} \begin{bmatrix} T_{a-1}(\theta) \\ T_a(\theta) \end{bmatrix} \tag{3}$$

the index is manipulated to get the results we want:

$$\begin{bmatrix} T_{a-1}(\theta) \\ T_a(\theta) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 2x \end{bmatrix} \begin{bmatrix} T_{a-2}(\theta) \\ T_{a-1}(\theta) \end{bmatrix} \tag{4}$$

Combining the above equations, we next get

$$\begin{bmatrix} T_a(\theta) \\ T_{a+1}(\theta) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 2\theta \end{bmatrix}^a \begin{bmatrix} T_0(\theta) \\ T_1(\theta) \end{bmatrix} \tag{5}$$

Where $$T_0(\theta) = 1, T_1(\theta) = \theta. \tag{6}$$

In addition, the Chebyshev polynomial possesses the following two intriguing properties:

- The property of a semi-group

$$\begin{aligned} T_r(T_s(\theta)) &= cos(rcos(s\, cos^{-1}(\theta))) \\ &= \cos\,(rscos^{-1}(\theta)) \\ &= T_{sr}(\theta) \\ &= T_s(T_r(\theta)) \end{aligned} \tag{7}$$

where r and s are both positive integers and $\theta \in [-1,1]$

- The property of a chaotic

An invariant density $f^*(\theta) = \frac{1}{\pi\sqrt{1-\theta^2}}$ is found in the Chebyshev map $T_a(\theta)$; $[-1,1 \longrightarrow [-1,1]]$ of degree $a > 1$, for positive Lyapunov exponent $\lambda = Ln(a) > 0$. Logistic maps can be constructed by using the Chebyshev map with *p=2*.

Since this condition holds under composition, the Chebyshev polynomials commute immediately.

$$T_r(T_s(\theta)) = T_s(T_r(\theta))$$

When it comes to Chebyshev polynomials, Zhang [15] has shown that the semi-group property applies for those defined on the interval $(-\infty, \infty)$ in order to make the formulas more secure. Polynomials in this form are called augmented Chebyshev polynomials.

$$T_n(\theta) = \left(2xT_{n-1}(\theta) - T_{n-2}(\theta)\right) (\text{mod } p) \tag{8}$$

where $n \geq 2, \theta \in (-\infty, \infty)$, and p is a large prime number. Obviously, one has

$$T_r(T_s(\theta))(\theta) = T_r(T_s(\theta)) = T_s(T_r(\theta))(\text{mod } p) \tag{9}$$

Theorem 1. **[14]** Let $f(u) = t^2 - 2ut + 1$ and α, β be two roots of $f(u)$. If u= $\frac{1}{2}(\alpha + \beta)$, in this case, the number of possible solutions is met by:

$$T_a(u) = \frac{(u+\sqrt{u^2-1})^a + (u-\sqrt{u^2-1})^a}{2} (\text{mod } p) \tag{10}$$

Theorem 2. **[14]** If a and b are two positive integers and $a > b$, then we obtain that:

$$2T_a(u).T_b(u) = T_{a+b}(u) + T_{a-b}(u) \tag{11}$$

Theorem 3. **[14]** If $a = b + c$ and p is a prime (i.e., large number), we obtain that:

$$\begin{aligned} &[T_a(u)]^2 + [T_b(u)]^2 + [T_c(u)]^2 \\ &= 2T_a(u)T_b(u)T_c(u) + 1(\text{mod } p) \end{aligned} \tag{12}$$

Lemma 1. **[14]** Let the elements of a finite field are g and h, i.e., if $g + g^{-1} = h + h^{-1}$then $g = h$ or

$$g = h^{-1}$$

Lemma 2. **[14]** For any $\alpha \in GF(p)$ and $y = \alpha^t$ for some integer t, we can find an integer $u \in GF(p)$ and then construct a chaotic maps sequence $\{T_a(u)\}$, in polynomial time such that

$$\frac{1}{2}(y + y^{-1}) = T_t(u) \in T_a(u) \quad (13)$$

Lemma 3. **[14]** Let p, n and α are the same as earlier; and G is the group formed by the combination of these three. To obtain the value of μ such that $a = T_{\mu^2(mod\ n)}(\alpha)\ mod\ p$, where a is given and $a \in G$, one must solve both the chaotic maps problem in G and the factorization of n.

Theorem 4: The discrete logarithm problem over $GF(p)$ can be solved in polynomial time if a method *AL* can be used to solve the chaotic mapping problem over GF).

2.2 The Factorization Problem.

Finding two huge integers *p* and *q* from a composite number *n*, which is the product of two numbers p and q, is known as the factorization problem. Large prime numbers aren't hard to come by, but factoring the product of two of them is regarded computationally challenging when the primes aren't randomly chosen. The RSA public-key cryptosystem was designed by Rivest et al. [16] because of the difficulties of this challenge. Many mathematicians have worked on the factorization problem for many years, but considerable progress has only been made in the last 20 years. Since the RSA cryptosystem was invented in 1978, several mathematicians have studied the topic in depth. Advanced algorithms could now be implemented and tested on high-performance computers. RSA has now been a problem for more than two decades [25]. More than a few studies on the problem's robustness have yielded attacks, while others evaded them. Based on the RSA problem, digital signatures and public-key encryption techniques have been created. What remains to be seen is how much of the RSA Issue's security is dependent on factoring, and whether, like with every cryptographic hard problem, more robust approaches than those currently available can ever be developed.

Definition 1: (FAC problem). Let n be a large composite integer with $n = rs$ where r and s are two large strong primes of 512-bits. Then find the primes $r$or s.

Definition 2: (QR problem). Let p, q be two strong primes of large size and γ is an integer. Then, compute γ such that $\gamma \equiv \beta^2 \bmod pq$

2.3 Computational Problem.

In order to demonstrate the security of our proposed cryptosystem, we show several essential mathematical features of Chebyshev chaotic maps:

a) The property of Semi-group: Given $\theta \in [-1,1]$,

$$T_r(T_s(\theta)) = \cos\left(r\cos^{-1}(s\cos^{-1}(\theta))\right)$$

$$= \cos\left(rs\cos^{-1}(\theta)\right)$$

$$= T_{sr}(\theta) = T_s(T_r(\theta))$$

b) An integer s must be found such that $T_s(\theta) = y$ in the discrete logarithm problem given as two elements x and y and an associated value for its value in the chaotic map.

c) If three elements x, $T_r(\theta)$, and $T_s(\theta)$, are given, the task of the Diffie-Hellman problem is to compute elements $T_{rs}(\theta)$.

3 The Proposed Scheme

The following parameters and notations will be used before the new scheme is introduced.

- Let p be a large prime and n is a factor of p−1 that is the product of two safe primes $\overline{p}$ and $\overline{q}$, i.e., $n = \overline{p}\overline{q}$
- Let α be an element in $GF(p)$ and the order of $\alpha$is n, and G is the multiplicative group generated by α. Note that the two large primes $\overline{p}$and$\overline{q}$, are kept secret for all users in the system.

3.1 Algorithm for Key Generation.

The following steps are taken during this phase.

- Select randomly integer b
- Compute the corresponding integers k such that
- Compute the corresponding integers K such that $K = T_{b^4}(\alpha)(\ mod\ n)$

The signer publishes his public keys as (p, n, K, α) and keeps his corresponding private keys as $(b, \overline{p}, \overline{q})$

3.2 Algorithm for Signing Message.

Our scheme's message-signing algorithm is presented in this section. Once the signer has decided on m (the message they want to sign), they subsequently compute the hashed value of it *h(r)*. Following are the steps that the signer must do in order to sign *h(r)*.

- Select a random integer $r \in \mathbb{Z}_n^*$
- Compute $L = T_{r^4}(\alpha)\ (mod\ p)$ (14)
- Calculate $S \equiv (h(m)\ b\ r\ L)\ mod\ n$ (15)
- Compute $\lambda \equiv (h(m)b + r\ L)^2\ mod\ n$ (16)

Signing the message *h(r)* is done by the original signer, who creates (L, S, λ).

3.3 Algorithm for Verifying Signature.

After the receiver received the message *h(r)* and signature from signer, he can verify the correctness and validity of the produced signature using the following verifying equation. If it holds, receiver is convinced the message was signed by the actual signer. Now we present the algorithm for verifying signature for our scheme.

- Compute$\gamma \equiv (\lambda^2 + 2S^2 - 4\lambda S)\ mod\ n$ (17)
- Compute

$$W_1 = \left[T_\gamma(\alpha)\right]^2 + \left[T_{h(m)^4 (mod\ n)}(K)\right]^2 + \left[T_{L^4 (mod\ n)}(L)\right]^2 mod\ p \quad (18)$$

- Calculate

$$W_2 = 2T_\gamma(\alpha)T_{h(m)^4 (mod\ n)}(K)\ T_{L^4 (mod\ n)}(L) + 1 \quad (19)$$

Accept the signature $(L, S,\ \lambda)$ as valid if and only if W_1=W_2.

Theorem 1: If the algorithms for generating keys and signing messages are run smoothly then the validation of signature in scheme is correct.

Proof: We have to show that the signature $(L, S,\ \lambda)$ satisfies $W_1 = W_2$. Note that

$$\lambda^2 = h(m)^4 b^4 + r^4 L^4 + 6(h(m) b\ r\ l)^2 + 4(h(m)^2 b^2 + r^2 L^2)\ h(m) b\ r\ L$$

$$= h(m)^4 b^4 + r^4 L^4 + 6S^2 + 4h(m) b\ r\ L(h(m)^2 b^2 + r^2 L^2)$$

$$= h(m)^4 b^4 + r^4 L^4 + 6\ S^2 + 4S(\lambda - 2S)$$

$$= h(m)^4 b^4 + r^4 L^4 6\ S^2 - 2S^2 + 4S\lambda$$

And also we have

$$\gamma \equiv (\lambda^2 + 2S^2 - 4\lambda S)\ mod\ n$$

$$\equiv h(m)^4 b^4 + r^4 L^4 - 2S^2 + 4S\lambda + 2S^2 - 4S\lambda$$

$$\equiv h(m)^4 b^4 + r^4 L^4$$

From Theorem. (3)

$$[T_a(m)]^2 + [T_b(m)]^2 + [T_c(m)]^2 = (2\ T_a(m) T_b(m) T_c(m) + 1)\ (mod\ p)$$

Let $a = h(m)^4 b^4 + r^4 L^4, c = h(m)^4 b^4,\ d = L^4 r^4$

Thus, we obtain

$$W_1 = \left[T_\gamma(\alpha)\right]^2 + \left[T_{h(m)^4 (mod\ n)}(K)\right]^2 + \left[T_{L^4 (mod\ n)}(L)\right]^2$$

$$= \left[T_{h(m)^4 b^4 + r^4 L^4}(\alpha)\right]^2 + \left[T_{h(m)^4 (mod\ n)} T_{b^4}(\alpha)\right]^2 + \left[T_{L^4 (mod\ n)} T_{r^4}(\alpha)\right]^2$$

$$= \left[T_{h(m)^4 b^4 + r^4 L^4}(\alpha)\right]^2 + \left[T_{h(m)^4 b^4 (mod\ n)}(\alpha)\right]^2 + \left[T_{L^4 r^4 (mod\ n)}(\alpha)\right]^2$$

$$= 2\ T_{h(m)^4 b^4 + r^4 L^4}(\alpha) T_{h(m)^4 b^4 (mod\ n)}(\alpha) T_{L^4 r^4 (mod\ n)}(\alpha) + 1$$

$$= 2T_\gamma(\alpha)T_{h(m)^4 (mod\ n)}(K)\ T_{L^4 (mod\ n)}(L) + 1 = W_2$$

4 Performance Analysis and Security Analysis

4.1 Security Analysis

We use heuristic security techniques to evaluate our system. It's done by looking at the various cryptographic attacks on the system by an attacker. The first step is to identify the various types of attacks and then analyze why each one would fail.

Attack 1. Adversary (Adv) wishes to obtain the secret keys of the scheme. In this case, Adv first analyzes (p, n, α) in order to recover the signer's private key b. He needs to solve $w \equiv T_{b^4 (mod\ n)}(\alpha)\ mod\ p$ which are clearly infeasible because the difficulty of solving CM and QR problems.

Attack 2. Adv tries to drive the signature $(L, S,\ \lambda)$ for given message m by letting two integers fixed and finding the other one. In this case, Adv randomly select $(S,\ \lambda)$ or (L, S) or (λ, L) and find L or λ or S respectively such that it satisfies $W_1 = W_2$.

Now say Adv fixes the values $(S,\ \lambda)$ and tries to figure out the value L, then using equations (18 and 19) as a starting point to solve the following equations.

$$\psi^2 - 2\psi T_\gamma(\alpha)T_{h(m)^4 (mod\ n)}(K) + \left[T_\gamma(\alpha)\right]^2 + \left[T_{h(m)^4 (mod\ n)}(K)\right]^2 - 1 = 0$$

As a result, ψ may be found using the following equation:

$$\psi = \frac{T_\gamma(\alpha)T_{h(m)^4 (mod\ n)}(k)}{2} \mp \frac{\sqrt{\left(\psi T_\gamma(\alpha)T_{h(m)^4 (mod\ n)}(K)\right)^2 + 4\left(\left[T_\gamma(\alpha)\right]^2 + \left[T_{h(m)^4 (mod\ n)}(K)\right]^2 - 1\right)}}{2}$$

Even if he can derive ψ from the preceding equation, finding L from $\psi = T_{L^4 (mod\ n)}(L)$ is impossible (i.e., infeasible). We can see from Lemma 1 that this is identical to solving the chaotic maps issue in *G* and factorizing *n*.

Adv may proceed this attack by selecting two integers

$(L,\ \lambda)$ and tries to figure out the value of S. So, since the Adv does not know the value of S, then γ cannot be found because$\gamma \equiv (\lambda^2 + 2S^2 - 4\lambda S)$. Then using equation (14) as a starting point to solve the following equations.

$$\omega^2 - 2\omega T_{h(m)^4(mod\ n)}(K)\ T_{L^4(mod\ n)}(L) + \left[T_{h(m)^4(mod\ n)}(K)\right]^2 + \left[T_{L^4(mod\ n)}(L)\right]^2 - 1 = 0$$

As a result, ω may be found using the following equation:

$$\omega = \frac{T_{L^4}(L)T_{h(m)^4(mod\ n)}(k)}{2} \mp \frac{\sqrt{\left(\omega T_{L^4}(L)T_{h(m)^4(mod\ n)}(K)\right)^2 + 4\left([T_{L^4}(L)]^2 + \left[T_{h(m)^4(mod\ n)}(K)\right]^2 - 1\right)}}{2}$$

Even if he can derive ω from the preceding equation, finding S from $\omega = T_\gamma(\alpha) = T_{(\lambda^2+2S^2-4\lambda S)(mod\ n)}(L)$ is impossible (i.e., infeasible). We can see from Lemma 1 that this is identical to solving the chaotic maps issue in G and factorizing n.

In the latter case also the same problem if the Adv selecting two integers $(L,\ S)$ and tries to figure out the value of λ. So, since the Adv does not know the value of λ, then γ cannot be found because $\gamma \equiv (\lambda^2 + 2S^2 - 4\lambda S)(\mathrm{mod}\ n)$, then using equations (18 and 19) as a starting point to solve the following equations.

Attack 3. Adv may also get a message signature M_j to obtain t a valid signature $(L_j,\ S_j,\ \lambda_j)$where $j = 1,2, \dots, t$ and tries to find the secret signature key. Here are Adv's equations.

$$\lambda_1^2 + 2S_1^2 - 4\lambda_1 S_1 = h(M_1)^4 b^4 + r_1^4 L_1^4\ (\mathrm{mod}\ n)$$

$$\lambda_2^2 + 2S_2^2 - 4\lambda_2 S_2 = h(M_2)^4 b^4 + r_2^4 L_2^4\ (\mathrm{mod}\ n)$$

$$\lambda_t^2 + 2S_t^2 - 4\lambda_t S_t = h(M_t)^4 b^4 + r_t^4 L_t^4\ (\mathrm{mod}\ n)$$

Where $j = 1,2, \dots, t$. The aforementioned t equations have $(t+1)$ variables, which are b and r_j. Because Adv can generate unlimited solutions to the given system of equations, it is impossible to determine which one is accurate.

Attack 4. Assume that Adv is able to solve QRP. That means, he can find the primes $(\bar{p}, \bar{q})$, but still does not know b^4 because the difficulty of solving CMP. Hence cannot obtain $b, s,$ and λ and fails to produce the signature$(L, S,\ \lambda)$.

Attack 5. Assume that Adv is able to solve CMP. That means, he can find the number b^4 but to get b be must face another problem, QRP which is hard to solve. Thus, he cannot compute the values $S \equiv (h(m)\ b\ r\ L)\ mod\ n$ and $\lambda \equiv (h(m)b + r\ L)^2\ (mod\ n)$ and fails to produce the signature $(L, S,\ \lambda)$.

4.2 Efficiency Performance

The Chebyshev polynomial computation problem, compared to RSA and ECC, has lower key sizes, faster computation, and less memory, energy, and bandwidth use. Scalar multiplications of elliptic curve exponentiations are unnecessary in our protocol. There are numerous ways to tackle the Chebyshev polynomial computation problem given by Wang [26]. For ease of reference, several notations for the procedures involved and their equivalent in seconds are supplied and defined as follows [3, 7, 20-21, 25, 28]:

- T_{exp} is the time in seconds for executing a modular exponentiation operation, $1T_{exp} \approx 5.37s$
- T_{mul} is the time for modular multiplication operation, $1T_{mul} \approx 0.00207s$
- $T_{ch}$is the time for executing a Chebyshev chaotic map operation, $1T_{ch} \approx 0.172$
- T_{inv} is the time complexity for evaluating a modular inverse computation, $T_{inv} \approx 10T_{mul} \approx 0.0207s$.

Table 1 shows a comparison between our approach and Chiou's system 2016, which is based on hybrid problems. Using the proposed technique, the total computational complexity is $6T_{mul} + 3T_{ch} + T_{inv}$, which is just 0:749 s, significantly less than the other schemes. Using chaotic maps and QR problems, we show that the suggested approach, based on DLP, QR, and FAC problems is more efficient.

5 Numerical Simulation of the Cryptosystem

Let say a signer wishes to sign a hashed message, *h(m)*=4. Let's consider $\bar{p} = 107, \bar{q} = 103$ and $p = 88169$, the modulus $n = \bar{p}\bar{q} = 11021$ and n is a factor of $p - 1$. We choose the numbers $b = 23$ and $\alpha = 55$ with order 11021 such that $55^{11021} = 1\ (\mathrm{mod}\ 88169)$, then compute the public key,

$$K = T_{23^4}(55) = T_{4316}(55) = 48096(\mathrm{mod}\ 88169)$$

Table 1: An evaluation based on their computational complexity-comparison

Scheme	Signature	Verification	Total (Seconds)	Hard Problems
Chiou's Scheme [13]	$3T_{exp} + 2T_{mul} + 2T_{sq}$	$4T_{exp} + T_{mul}$	42.9993	DLP, FAC
Proposed Scheme	$5T_{mul} + T_{ch} + 3T_{sq} + T_h$	$7T_{sq} + 3T_{ch} + T_h + 3T_{mul}$	0.749	Chaotic map, QR

Thus our public key and secret key of the scheme are$(88169,11021,48096,55)$ and 107, 103, 2, respectively. To sign, the signer first chooses at random $r = 13 \in \mathbb{Z}_n^*$ and computes the following:

$$L = T_{13^4}(55)(\text{mod } 88169) = 80445 \text{ (mod } 88169)$$

$$S \equiv 402(13)(23)(80445)(\text{mod } 1102) \equiv 9676 \text{ (mod } 1102)$$

$$\lambda \equiv (402 \times 23 + 13 \times 80445)^2(\text{mod } 1102) \equiv 5257 \text{ (mod } 1102)$$

The signature produces as (L, S, λ) = (88169,1102,525). To test its validity, the verifier calculates the following:

$$\gamma \equiv (\lambda^2 + 2S^2 - 4\lambda S)$$

$$\equiv (5257^2 + 2 \times 9676^2)$$

$$- 4 \times 5257 \times 9676(\text{ mod } 1102)$$

$$\equiv 1317 \text{ (mod } 1102)$$

$$W_1 = \left[T_\gamma(\alpha)\right]^2 + \left[T_{h(m)^4(mod\ n)}(K)\right]^2$$

$$+\left[T_{L^4(mod\ n)}(L)\right]^2\ mod\ p$$

$$W_1 = [T_{1317}(55)]^2 + [T_{528}(55)]^2$$

$$+[T_{789}(55)]^2\ (mod\ 88169)$$

$$W_1 = [73392]^2 + [86390]^2 + [3092]^2$$

$$W_1 = 82254 \text{ (mod } 88169)$$

$$W_2 = 2 \times 73392 \times 86390 \times 3092 + 1$$

$$W_2 = 82254$$

Since W1=W2 then the signature is now validated

6 Conclusion

Based on chaotic maps and quadratic residue problems, we developed a novel signature technique. Using chaotic maps, the proposed system claims to give much improved performance than existing signature schemes based on FAC and DL problems. The proposed strategy has a significantly reduced calculation cost than previous schemes, resulting in enhanced security, dependability, and productivity.

References

[1] O. M. Al-Hazaimeh, "A New Dynamic Speech Encryption Algorithm Based on Lorenz Chaotic Map over Internet Protocol," *International Journal of Electrical and Computer Engineering*, 10(5):4824, 2020.

[2] O. M. Al-hazaimeh, "A New Speech Encryption Algorithm Based on Dual Shuffling Hénon Chaotic Map," *International Journal of Electrical and Computer Engineering (IJECE)*, 11(3):2203-2210, 2021.

[3] O. M. Al-Hazaimeh, A. A. Abu-Ein, K. M. Nahar, and I. S. Al-Qasrawi, "Chaotic Elliptic Map for Speech Encryption," *Indonesian Journal of Electrical Engineering and Computer Science*, 25(2):1103-1114, 2022.

[4] L. Bakrawy, N. Ghali, A. Hassanien and Th. Kim, A Fast and Secure One-Way Hash Function," *Compututer and Information Science*, 259:85-93, 2011.

[5] K. Chain and C. Kuo, "A New Digital Signature Scheme Based on Chaotic Maps," *Nonlinear Dynamics*, 24(4):1003-1012, 2013.

[6] S. Chiou, "Novel Digital Signature Schemes Based on Factoring and Discrete Logarithms," *International Journal of Security and Its Applications*, 10(3):295-310, 2016.

[7] S. Ghassan, "Certificate Revocation Management in VANET," *International Journal of Cyber-Security and Digita,* 1(2):115-121, 2012.

[8] H. He, "Digital Signature Schemes Based on Factoring and Discrete Logarithms," *Electronics Letters*, 37(4):220-222, 2001.

[9] S. Hung, "Cryptanalysis of a Digital Signature Scheme Based on Factoring and Discrete Logarithms," *Proceedings of the National Computer Symposium*, Taipei, Taiwan, F043- F045, 2001.

[10] S. Hwang, C. Yang, and F. Tzeng, "Improved Digital Signature Scheme Based on Factoring and Discrete Logarithms," *Journal of Discrete Mathematical Sciences and Cryptography,* 5(2):151-155, 2022.

[11] E. Ismail and N. Tahat, "A New Signature Scheme Based on Multiple Hard Number Theoretic Problems," *International Scholarly Research Notices*, Article ID 231649, vol. 2011, 3 pages, 2011.

[12] E. Ismail, N. Tahat, and R. Ahmad, "A New Digital Signature Scheme Based on Factoring and Discrete Logarithms*, Journal of Mathematics and Statistics,* 14(4):222-225, 2008.

[13] X. Li and D. Zhao, "Optical Color Image Encryption with Redefined Fractional Hartley Transform," *International Journal for Light and Electron Optics*, 121(7):673- 677, 2010.

[14] R. Matthews, "On the Derivation of a Chaotic Encryption Algorithm," *Cryptologia*, 13(1):29-41, 1989.

[15] A. K. Mohammad, P. M. Himadri, and D. J. Syeda, "Anti-Synchronization Phenomenon of Discrete Chaotic Maps using Linear Transformations," *Journal of Information and Optimization Sciences*, 41(8):1757-1769, 2020.

[16] F. Pon, H. Lu, and B. Jeng, "Meta-He Digital Signature Schemes Based on Factoring and Discrete Logarithms," *Applied Mathematics and Computation*, 65(1):171-176, 2005.

[17] H. Qian, F. Cao, and H. Bao, "Cryptanalysis of LiTzeng Hwang Improved Signature Schemes Based on Factoring and Discrete Logarithms," *Applied*

Mathematics and Computation, 166(3):501-505, 2005.
[18] A. Shakiba, "Security Analysis for Chaotic Maps-Based Mutual Authentication and Key Agreement using Smart Cards for Wireless Networks," *Journal of Information and Optimization Sciences*, 40(3):725-750, DOI: 10.1080/02522667.2018.1470752, 2019.
[19] Z. Shao, "Digital Signature Schemes Based on Factoring and Discrete Logarithms," *Electronics Letters*, 38(24):1518-1519, 2002.
[20] N. Tahat, "Convertible Multi-Authenticated Encryption Scheme with Verification Based on Elliptic Curve Discrete Logarithm Problem," *Int. J. Computer Applications in Technology*, 54(3):229-235, 2016.
[21] N. Tahat, A. K. Alomari, A. Al–Freedi, O. M. Al-Hazaimeh, and M. F. Al–Jamal, "An Efficient Identity-Based Cryptographic Model for Chebyhev Chaotic Map and Integer Factoring Based Cryptosystem," *Journal of Applied Security Research*, 14(3):257-269, 2019.
[22] N. Tahat, A. K. Alomari, O. M. Al-Hazaimeh, and M. F. Al-Jamal, An Efficient Self-Certified Multi-Proxy Signature Scheme Based on Elliptic Curve Discrete Logarithm Problem," *Journal of Discrete Mathematical Sciences and Cryptography*, 23(4):935-948, 2020.
[23] J. Tay, C. Quan, W. Chen, and Y. Fu, "Color Image Encryption Based on Interference and Virtual Optics," *Optics and Laser Technology*, 142(2):409-415, 2010.
[24] C. Wang, H. Lin, and C. Chang, "Signature Scheme Based on Two Hard Problems Simultaneously," *Proceedings of the 17th International Conference on Advanced Information Networking and Application (AINA),* Xian, China, pp. 557-560, 2003.
[25] X. Wang, X. Wang, and J. Zhao, "Chaotic Encryption Algorithm Based Alternant of Stream Cipher and Block Cipher," *Nonlinear Dyn*., 63:587-597, 2011.
[26] L. Xiong, N. Jianwei, K. Saru, H. Sk, W. Fan, K. Muhammad, and K. Ashok, "A Novel Chaotic Maps-Based User Authentication and Key Agreement Protocol for Multisever Environments with Provable Security, *Wireless Pers Communication*, 89(2):569-597, 2016.
[27] J. Yoon and S. Jeon, "An Efficient and Secure Diffie-Hellman Key Agreement Protocol Based on Chebyshev Chaotic Map," *Journal of Communications in Nonlinear Science and Numerical Simulation*, 16(6):2383-2389, 2011.
[28] L. Zhang, "Cryptanalysis of the Public Key Encryption Based on Multiple Chaotic Systems," *Chaos Solitons Fractals*, 37(3):669-674, 2008.

Rania Shaqbou'a received the B.Sc. degree in mathematics from Yarmouk University, Jordan, in 1999, the M.Sc. degree in Pure Mathematics from University of Jordan, in 2005. She is an Assistant Lecturer at Department Mathematics, Hashemite University.

Nedal M. Tahat received his BSc in Mathematics at the Yarmouk University, Jordan, in 1994, and MSc in Pure Mathematics at Al al-Bayt University, Jordan, in 1998. He is a PhD candidate in Applied Number Theory (Cryptography) from the National University of Malaysia (UKM), in 2010. He is a Full Professor at the Department Mathematics, Hashemite University. His main research interests are cryptology and number theory. He has published more than 52 papers, authored/co-authored, and more than 15 refereed journal and conference papers. He can be contacted at email: nedal@hu.edu.jo

Osama Ababneh is an Assistant Professor of Applied Mathematics at the Faculty of Science, Mathematics department, Zarqa University, Jordan. In 2005 Ababneh got his first degree in Mathematics at Al-Albyet University and from 2007 to 2010 he carried out further studies in Mathematics (Master and PHD) at UKM University, Malaysia. From 2011 till now he has been an Assistant Professor at the Irbed University and Zarqa university, Jordan. Ababneh is the Editor in Chief of General Letters in Mathematics. Ababneh has more than twenty scientific papers and is a member of scientific committees of various international conferences and an editorial board member of various scientific journals.

Obaida M. Al-Hazaimeh earned a BSc in Computer Science from Jordan's Applied Science University in 2004 and an MSc in Computer Science from Malaysia's University Science Malaysia in 2006. In 2010, he earned a PhD in Network Security (Cryptography) from Malaysia. He is a Full professor at Al-Balqa Applied University's Department of Computer Science and Information Technology. Cryptology, image processing, machine learning, and chaos theory are among his primary research interests. He has published around 51 papers in international refereed publications as an author or co-author. He can be contacted at email: dr_obaida@bau.edu.jo

Time Complexity Analysis for Cullis/Radic and Dodgson's Generalized/Modified Method for Rectangular Determinants Calculations

Armend Salihu*,Halil Snopce*, Artan Luma*, Jaumin Ajdari*
South East European University, Tetovo, NORTH MACEDONIA.

Abstract

In this paper we present an analysis of the time complexity of algorithms based on Cullis/Radic Definition and Dodgson's Generalized/Modified Method for calculating rectangular/non-square determinants. We have identified the asymptotic time complexity of these algorithms, and that both algorithms have their advantages in relation to time complexity. From the time complexity analysis, we observed that the Cullis/Radic definition has an asymptotic time complexity of $O(C\binom{m}{n} \cdot m^3)$, while Dodgson's Generalized/Modified Method has an asymptotic time complexity of $O(2^{2m} \cdot (n-m)^2)$. Further, we noticed that in cases where the number of rows is less than or equal to half the number of columns, it is more appropriate to use the algorithm based on Dodgson's Generalized/Modified Method, while in cases where the number of rows is greater than half the number of columns, then Cullis/Radic Definition based algorithm is more suitable to use. Based on this analysis, we have also presented an algorithm which is a combination of these two algorithms and depending on the ratio between the number of rows and columns the rectangular determinant is calculated with the most appropriate method, for which we calculated the worst-case asymptotic time complexity as $O(\frac{n!}{((n/2)!)^2} \cdot \frac{n}{2}^3)$ while the best-case asymptotic time complexity is calculated as $O(n^3)$

Key Words: Rectangular determinants; time complexity; Dodgson's method; pivotal condensation; execution time.

1 Cullis/Radic and Generalized/Modified Dodgson's Method for Rectangular Determinants Calculation

The following presents the determinant calculation method based on the Cullis/Radic definition:

Theorem 1. *Let A be $m \times n$ a rectangular matrix:*

$$A_{m\times n} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}. \quad (1)$$

Its determinant, where $m \leq n$ is the sum (See: [4] [8]):

$$det(A_{m\times n}) = |A_{m\times n}| = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{vmatrix}$$

$$= \sum_{1<j_1<\cdots<j_m<n} (-1)^{r+s} \begin{vmatrix} a_{1j_1} & a_{1j_2} & \cdots & a_{1j_n} \\ a_{2j_1} & a_{2j_2} & \cdots & a_{2j_n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{mj_1} & a_{mj_2} & \cdots & a_{mj_n} \end{vmatrix}. \quad (2)$$

where $r = 1 + \cdots + m, s = j_1 + \cdots + j_m$.

Proof. See definition 1 in [8]. □

The following the pseudocode of the algorithm based on the above-mentioned method for calculating determinant of rectangular matrices.

P 1: Algorithm (det_A) based on Cullis-Radic method to calculate rectangular determinants

Step 1: Identify all combinations for determining m×m square determinants from columns combinations:
if $m = n$
Calculate square determinant with known methods.
else
$$B = nchoosek(1:n,m);$$

Step 2: Identify all square determinants from the combination of columns:
Create loop from 1 to total number of combinations (length of vector B)
$$D\{i\} = A(1:m, B(i,1:m)));$$

Step 3: Calculate determinants of square blocks from D
Create loop from 1 to total number of combinations (length of vector B)
$$d = d + (-1)\hat{}(sum(1:m) + sum(B(i,1:m))) * SquareDet(D\{i\});$$

Step 4: Display the result of the determinant

* Faculty of Contemporary Sciences and Technologies,
Emails: as28364@seeu.edu.mk, h.snopce@seeu.edu.mk,
a.luma@seeu.edu.mk, and j.ajdari@seeu.edu.mk.

Theorem 2. *(Generalized Dodgson's formula) [2] Let A be $m \times n$ a rectangular matrix. Then for $p = min(m,n) \geq 2$, we have:*

$$\begin{aligned} & det\left(A_{\substack{1\leq i\leq m\\ 1\leq j\leq n}}\right)\cdot det\left(A_{\substack{i\neq m-1,m\\ j\neq n-1,n}}\right) \\ = & \underset{(\varepsilon,p-1)}{det}\left(A_{\substack{1\leq i<m\\ 1\leq j<n}}\right)\cdot \underset{(\varepsilon,p-1)}{det}\left(A_{\substack{1<i\leq m\\ 1<j\leq n}}\right) \\ - & \underset{(\varepsilon,p-1)}{det}\left(A_{\substack{1\leq i<m\\ 1<j\leq n}}\right)\cdot \underset{(\varepsilon,p-1)}{det}\left(A_{\substack{1<i\leq m\\ 1\leq j<n}}\right) \\ + & \underset{(\varepsilon,p)}{det}\left(A_{\substack{1\leq i\leq m\\ 1<j<n}}\right)\cdot \underset{(\varepsilon,p-2)}{det}\left(A_{\substack{1<i<m\\ 1\leq j\leq n}}\right) \end{aligned} \tag{3}$$

Proof. See theorem 5.1 in [2]. □

In the following, we have developed the computer algorithm $(det\_Dodgson)$ for theorem 1.

Since this method is applied for $m \geq 3$, and $m \leq n-2$, m-number of rows, n-number of columns of the matrix. The following is presented on the pseudocode of theorem 1.

P 2: Algorithm $(det\_Dodgson)$ for generalized Dodgson method to calculate rectangular determinants

Step 1: Checking for conditions:
if $m < 3$ or $m = n-1$
Calculate rectangular determinant with known methods, like Laplace, Radic, Chios-like, etc.
else if $m = n$
Calculate square determinant with known methods.
else
Step 2: Calculate submatrices:
Calculate submatrices presented on theorem 1, calling *det_Dodgson* algorithm until the conditions of step 1 are met, as following:

$$\begin{aligned} d1 &= det\_Dodgson(A(1:m-1,1:n-1)); \\ d2 &= det\_Dodgson(A(1:m-1,2:n)); \\ d3 &= det\_Dodgson(A(2:m,1:n-1)); \\ d4 &= det\_Dodgson(A(2:m,2:n)); \\ d5 &= det\_Dodgson(A(2:m-1,1:n)); \\ d6 &= det\_Dodgson(A(1:m,2:n-1)); \\ d7 &= det\_Dodgson(A(2:m-1,2:n-1)); \end{aligned}$$

Step 3: After calculating submatrices, calculate the result of the determinant as following:

$$d = (d1*d4 - d2*d3 + d5*d6)/d7;$$

Recently, in 2022 we identified 9 different cases of Dodgson's generalization formula for rectangular determinant calculation, which is provided in theorem 3.

Theorem 3. *[10] The pivot block $\underset{(\varepsilon,p-1)}{det}\left(A_{\substack{1<i<m\\ 1<j<n}}\right)$ of Bayat's formula can be any block of order $(m-2)\times(n-2)$ from the given determinant, and the following cases are:*

Case 1: Pivot block is: $\underset{(\varepsilon,p-1)}{det}\left(A_{\substack{1\leq i\leq m-2\\ 1\leq j\leq n-2}}\right)$
Case 2: Pivot block is: $\underset{(\varepsilon,p-1)}{det}\left(A_{\substack{1\leq i\leq m-2\\ 2\leq j\leq n-1}}\right)$
Case 3: Pivot block is: $\underset{(\varepsilon,p-1)}{det}\left(A_{\substack{1\leq i\leq m-2\\ 3\leq j\leq n}}\right)$
Case 4: Pivot block is: $\underset{(\varepsilon,p-1)}{det}\left(A_{\substack{2\leq i\leq m-1\\ 1\leq j\leq n-2}}\right)$
Case 5: Pivot block is: $\underset{(\varepsilon,p-1)}{det}\left(A_{\substack{2\leq i\leq m-1\\ 2\leq j\leq n-1}}\right)$
Case 6: Pivot block is: $\underset{(\varepsilon,p-1)}{det}\left(A_{\substack{2\leq i\leq m-1\\ 3\leq j\leq n}}\right)$
Case 7: Pivot block is: $\underset{(\varepsilon,p-1)}{det}\left(A_{\substack{3\leq i\leq m\\ 1\leq j\leq n-2}}\right)$
Case 8: Pivot block is: $\underset{(\varepsilon,p-1)}{det}\left(A_{\substack{3\leq i\leq m\\ 2\leq j\leq n-1}}\right)$
Case 9: Pivot block is: $\underset{(\varepsilon,p-1)}{det}\left(A_{\substack{3\leq i\leq m\\ 3\leq j\leq n}}\right)$

Proof. See theorem 3 in [10]. □

The pseudocode of each case from theorem 2 is like pseudocode presented in P 2, and changes in steps 2 for each case. For example, the pseudocode for case 1 is changed as following:

P 3: Modified algorithm (*det_Blocks*) based on theorem 2 (as example is considered case 1)

Step 1: Checking for conditions:
if $m < 3$ or $m = n-1$
Calculate rectangular determinant with known methods, like Laplace, Radic, Chios-like, etc.
else if $m = n$
Calculate square determinant with known methods.
else
Step 2: Calculate submatrices:
Calculate submatrices presented on theorem 1, calling *det_Dodgson* algorithm until the conditions of step 1 are met:

$$\begin{aligned} d1 &= det\_Blocks(A(1:m-1,1:n-1)); \\ d2 &= det\_Blocks(A(1:m-1,[1:n-2 \quad n])); \\ d3 &= det\_Blocks(A([1:m-2 \quad m],1:n-1)); \\ d4 &= det\_Blocks(A([1:m-2 \quad m],[1:n-2 \quad n])); \\ d5 &= det\_Blocks(A(1:m-2,1:n)); \\ d6 &= det\_Blocks(A(1:m,1:n-2)); \\ d7 &= det\_Blocks(A(1:m-2,1:n-2)); \end{aligned}$$

Step 3: After calculating submatrices, calculate the result of the determinant as following:

$$d = (d1 * d4 - d2 * d3 + d5 * d6)/d7;$$

The pseudocode presented in P 3 represents case 1 of theorem 2. However, the same algorithm can be used for each case of theorem 2, with changes in step 2 while selecting pivot block and reflecting that pivot block in each submatrix.

The above-mentioned theorem and pseudocode, has its advantage in cases of matrices with several zero elements. We have developed the algorithm that finds pivot block with highest number of zero elements, which is presented in pseudocode P 4 [10].

P 4: Find the block of order $(m-2) \times (n-2)$ with highest number of zero elements

Step 1: Insert the rectangular determinant A
Step 2: Calculate number of nonzero elements for each row/column
Initialize R for rows and C for columns
Create loop for i from 1 to m
Create loop for j from 1 to n
if $A(i,j) \neq 0$

$$R(i) = R(i) + 1;$$
$$C(i) = C(i) + 1;$$

Step 3: Find the best case with the highest number of zero elements
Initialize first case: $k = 1$
if $C(2) + C(n-1) < C(1) + C(n)$

$$k = 2;$$

else if $C(1) + C(2) < C(n-1) + C(n)$

$$k = 3;$$

if $R(2) + R(m-1) < R(1) + R(m)$

$$k = k + 3;$$

else if $R(1) + R(2) > R(m-1) + R(m)$

$$k = k + 6;$$

Step 4: Return best case

2 Time Complexity Analysis

In the following we present the time complexity analysis of the above-mentioned algorithms [7] [12] [9] [3].

Time complexity analysis of function (det_A) of algorithm P 1, based on Cullis-Radic method, is presented in Table 1.

Table 1: Time complexity of det_A function

Function: det_A		**Cost**	**time**
$[m,n] = size(A);$		$T_1 = const_1$	1
$d = 0;$		$T_2 = const_2$	1
if $m == n$ $d = det(A);$		$T_3 = n^3$	1
else	$B = nchoosek(1:n,m);$	$T_4 = const_4$	1
	for $i = 1 : length(B)$ d=d+ (-1)^(sum(1:m) +sum(B(i,[1:m]))) *det((A([1:m],[B(i,[1:m])])); end	There are several methods to calculate square determinants with different time complexity, however we will be based on LU factorization method [16]: $T_4 = m^3$	$C\binom{n}{m}$

Based on Table 1, we have:

$$Total\_Cost = 1 \cdot T_1 + 1 \cdot T_2 + 1 \cdot T_3 + Max(1 \cdot T_4, C\binom{n}{m} \cdot T_4)$$

$$= 1 \cdot const_1 + 1 \cdot const_2 + 1 \cdot const_3 + Max(1 \cdot n^3, C\binom{n}{m} \cdot m^3).$$

Hence, the highest order is $C\binom{n}{m} \cdot m^3$. After eliminating constants, the asymptotic time complexity is $O(C\binom{n}{m} \cdot m^3)$.

Time complexity analysis of function $(det\_Dodgson)$ of algorithm P 2, based on Dodgson's generalized method provided by Bayat, is presented in Table 2.

Table 2: Time complexity of *det_Dodgson* function

Function: *det_Dodgson*		**Cost**	**Times**
[m,n] = size(A);		$T_1 = const_1$	1
if m==n d=det(A);		$T_2 = n^3$	1
if m==n-1 $d = det\_Ones(A)$;		Based on Algorithm 2.2 (See [11]), transforms determinant of order $(n-1)\times n$ to $n\times n$ by adding one row of elements equal to 1. Square determinant's time complexity is $T_3 = O(n^3)$.	1
else if $m < 3$ $d = det\_A(A)$;		As it is calculated the det_A time complexity is: $T_4(3,n) = C\binom{n}{3}\cdot 3^3 = \frac{n\cdot(n-1)\cdot(n-2)\cdot(n-3)!}{3!\cdot(n-3)!}\cdot 3^3$ $= n\cdot(n-1)\cdot(n-2)\cdot 4.5 \approx n^3$.	1
else	$d1 = det\_Dodgson(A(1:m-1,1:n-1))$; $d2 = det\_Dodgson(A(1:m-1,2:n]))$; $d3 = det\_Dodgson(A(2:m,1:n-1))$; $d4 = det\_Dodgson(A(2:m,2:n]))$;	$T_{5-1}(m,n) = 4\cdot T_{5-1}(m-1,n-1)+1$, $T_{5-1}(m-1,n-1) = 4\cdot T_{5-1}(m-1-1,n-1-1)+1$ $= 4\cdot T_{5-1}(m-2,n-2)+1$, $T_{5-1}(m,n) = 4\cdot(4\cdot(T_{5-1}(m-2,n-2))+1+1$ $= 4^2\cdot T_{5-1}(m-2,n-2)+2$ for any k, we have: $T_{5-1}(m,n) = 4^k\cdot T_{5-1}(m-k,n-k)+k$, for $m-k=2 \Rightarrow k=m-2$, $T_{5-1}(m,n) = 4^{m-2}\cdot T_{5-1}(1,n-m+2)+m-2$ Based on the first condition: $T_{5-1}(2,n-m+2 = C\binom{n-m+2}{2}\cdot 2^3$ $\frac{(n-m+2)\cdot(n-m+1)}{2}\cdot 2^3 = 4\cdot(n-m+2)\cdot(n-m+1)$. $T_{5-1}(m,n) = 4^{m-2}\cdot 4\cdot(n-m+2)\cdot(n-m+1)+m-2$ $\approx 4_{m-1}\cdot(n-m+2)\cdot(n-m+1)$.	
	$d5 = det\_Dodgson(A(2:m-1,1:n))$;	$T_{5-2}(m,n) = T5-2(m-1,n-1)+1$, $T_{5-2}(m-1.n-1) = T_{5-2}(m-1-1,n-1-1)+1$ $= T_{5-2}(m-2,n-2)+1$, $T_{5-2}(m,n) = T_{5-2}(m-2,n-2)+1+1 = T_{5-2}(m-2,n-2+2$, for any k, we have: $T_{5-2}(m,n) = T_{5-2}(m-k,n-k)+k$, for $m-k=2 \Rightarrow k=m-2$, $T_{5-2}(m,n) = T_{5-2}(2,n-m-+2)+m-2$. Based on first condition: $T_{5-2}(2,n-m+2) = C\binom{n-m+2}{2}\cdot 2^3 = \frac{(n-m+2)\cdot(n-m+1)}{2}\cdot 2^3$ $= 4\cdot(n-m+1)\cdot(n-m+1)$. $T_{5-2}(m,n) = 4\cdot(n-m+2)\cdot(n-m+1)+m-2$ $\approx 4\cdot(n-m+2)\cdot(n-m+1)$.	
	$d6 = det\_Dodgson(A(1:m,2:n-1))$;	$T_{5-3}(m,n) = T_{5-3}(m,n-1)+1$, $T_{5-3}(m,n-1) = T_{5-3}(m,n-1-1)+1 = T_{5-3}(m,n-2)+1$, $T_{5-3}(m,n) = T_{5-3}(m,n-2)+1+1 = T_{5-3}(m,n-2)+2$, for any k, we have: $T_{5-3}(m,n) = T_{5-3}(m,n-k)+k$, for $n-k=m+1 \Rightarrow k=n-m-1$, $T_{5-3}(m,n) = T_{5-3}(m,n-n+m+1)+n-m-1$ $= T_{5-3}(m,m+1)+n-m-1$. Based on first condition: $T_{5-3}(m,m+1) = C\binom{m+1}{m}\cdot m^3 = (m+1)\cdot m^3 = m^4+m^3$. $T_{5-3}(m,n) = m^4+m^3+n-m-1 \approx m^4$.	

	$d7 = det\_Dodgson(A(2:m-1,2:n-1));$	$T_{5-4}(m,n) = T_{5-4}(m-2,n-2)+1,$ $T_{5-4}(m-2,n-2) = T_{5-4}(m-2-2,n-2-2)+1$ $= T_{5-4}(m-4,n-4)+1$ $T_{5-4}(m,n) = T_{5-4}(m-4,n-4)+1+1 = T_{5-4}(m-4,n-4)+2,$ for any k, we have: $T_{5-4}(m,n) = T_{5-4}(m-k,n-k) = \frac{k}{2},$ for $m-k=2 \Rightarrow k = m-2,$ $T_(m,n) = T_{5-4}(2,n-m+2)+\frac{m}{2}-2.$ Based on first condition: $T_{5-4}(2,n-m+2) = C\binom{n-m+2}{2}\cdot 2^3 = \frac{(n-m+1)\cdot(n-m+1)}{2}\cdot 2^3$ $= 4\cdot(n-m+2)\cdot(n-m+1).$ $T_{5-4}(m,n) = 4\cdot(n-m+2)\cdot(n-m+1)+\frac{m}{2}-2$ $\approx 4\cdot(n-m+2)\cdot(n-m+1).$	
$T_5 = T_{5-1}+T_{5-2}+T_{5-3}+T_{5-4} = 4^{m-1}\cdot(n-m+2)\cdot(n-m+1)+4\cdot(n-m+2)\cdot(n-m+1)+m^4+4$ $\cdot(n-m+2)\cdot(n-m+1 \approx 4^{m-1}\cdot(n-m+2)\cdot(n-m+1).$			1
$d = (d1*d4-d2*d3+d5*d6)/d7;$		$T_6 = const_6$	1

Based on Table 2, we have:

$$Total\_Cost = 1\cdot T_1 + Max(1\cdot T_2, 1\cdot T_3, 1\cdot T_4, 1\cdot T_5)+1\cdot T_6$$
$$= 1\cdot Const_1 + Max(1\cdot n^3, 1\cdot n^3, 1\cdot n^3, 1\cdot 4^{m-1}$$
$$\cdot(n-m+2)\cdot(n-m+1))+1\cdot Const_6.$$

Hence, the highest order is $4^{m-1}\cdot(n-m+2)\cdot(n-m+1)$. After eliminating constants and other lower grades, we can summarize the asymptotic time complexity as $O(2^2 m\cdot(n-m)^2)$.

Time complexity analysis of function (*det_Blocks*) of algorithm P 3, based on modified Dodgson's generalized method, is presented in Table 3.

Table 3: Time complexity of *det_Blocks* function

Function: *det_Blocks*		**Cost**	**Times**
[m,n] = size(A);		$T_1 = const_1$	1
if m==n d=det(A);		$T_2 = n^3$	1
if m==n-1 $d = det\_Ones(A);$		Based on Algorithm 2.2 (See [11]), transforms determinant of order $(n-1)\times n$ to $n\times n$ by adding one row of elements equal to 1. Square determinant's time complexity is $T_3 = O(n^3)$.	1
else if $m<3$ $d = det\_A(A);$		As it is calculated the *det_A* time complexity is: $T_4(3,n) = C\binom{n}{3}\cdot 3^3 = \frac{n\cdot(n-1)\cdot(n-2)\cdot(n-3)!}{3!\cdot(n-3)!}\cdot 3^3$ $= n\cdot(n-1)\cdot(n-2)\cdot 4.5 \approx n^3.$	1
else	$d1 = det\_Blocks(A(1:m-1,1:n-1));$ $d2 = det\_Blocks(A(1:m-1,2:n]));$ $d3 = det\_Blocks(A(2:m,1:n-1));$ $d4 = det\_Blocks(A(2:m,2:n]));$	$T_{5-1}(m,n) = 4\cdot T_{5-1}(m-1,n-1)+1,$ $T_{5-1}(m-1,n-1) = 4\cdot T_{5-1}(m-1-1,n-1-1)+1$ $= 4\cdot T_{5-1}(m-2,n-2)+1,$ $T_{5-1}(m,n) = 4\cdot(4\cdot(T_{5-1}(m-2,n-2))+1+1$ $= 4^2\cdot T_{5-1}(m-2,n-2)+2$ for any k, we have: $T_{5-1}(m,n) = 4^k\cdot T_{5-1}(m-k,n-k)+k,$ for $m-k=2 \Rightarrow k = m-2,$ $T_{5-1}(m,n) = 4^{m-2}\cdot T_{5-1}(1,n-m+2)+m-2$ Based on the first condition: $T_{5-1}(2,n-m+2 = C\binom{n-m+2}{2}\cdot 2^3$ $\frac{(n-m+2)\cdot(n-m+1)}{2}\cdot 2^3 = 4\cdot(n-m+2)\cdot(n-m+1).$ $T_{5-1}(m,n) = 4^{m-2}\cdot 4\cdot(n-m+2)\cdot(n-m+1)+m-2$ $\approx 4_{m-1}\cdot(n-m+2)\cdot(n-m+1).$	

	$d5 = det\_Blocks(A(2:m-1,1:n));$	$T_{5-2}(m,n) = T5-2(m-1,n-1)+1,$ $T_{5-2}(m-1.n-1) = T_{5-2}(m-1-1,n-1-1)+1$ $= T_{5-2}(m-2,n-2)+1,$ $T_{5-2}(m,n) = T_{5-2}(m-2,n-2)+1+1 = T_{5-2}(m-2,n-2+2,$ for any k, we have: $T_{5-2}(m,n) = T_{5-2}(m-k,n-k)+k,$ for $m-k=2 \Rightarrow k=m-2,$ $T_{5-2}(m,n) = T_{5-2}(2,n-m-+2)+m-2.$ Based on first condition: $T_{5-2}(2,n-m+2) = C\binom{n-m+2}{2}\cdot 2^3 = \frac{(n-m+2)\cdot(n-m+1)}{2}\cdot 2^3$ $= 4\cdot(n-m+1)\cdot(n-m+1).$ $T_{5-2}(m,n) = 4\cdot(n-m+2)\cdot(n-m+1)+m-2$ $\approx 4\cdot(n-m+2)\cdot(n-m+1).$	
	$d6 = det\_Blocks(A(1:m,2:n-1));$	$T_{5-3}(m,n) = T_{5-3}(m,n-1)+1,$ $T_{5-3}(m,n-1) = T_{5-3}(m,n-1-1)+1 = T_{5-3}(m,n-2)+1,$ $T_{5-3}(m,n) = T_{5-3}(m,n-2)+1+1 = T_{5-3}(m,n-2)+2,$ for any k, we have: $T_{5-3}(m,n) = T_{5-3}(m,n-k)+k,$ for $n-k=m+1 \Rightarrow k=n-m-1,$ $T_{5-3}(m,n) = T_{5-3}(m,n-n+m+1)+n-m-1$ $= T_{5-3}(m,m+1)+n-m-1.$ Based on first condition: $T_{5-3}(m,m+1) = C\binom{m+1}{m}\cdot m^3 = (m+1)\cdot m^3 = m^4+m^3.$ $T_{5-3}(m,n) = m^4+m^3+n-m-1 \approx m^4.$	
	$d7 = det\_Blocks(A(2:m-1,2:n-1));$	$T_{5-4}(m,n) = T_{5-4}(m-2,n-2)+1,$ $T_{5-4}(m-2,n-2) = T_{5-4}(m-2-2,n-2-2)+1$ $= T_{5-4}(m-4,n-4)+1$ $T_{5-4}(m,n) = T_{5-4}(m-4,n-4)+1+1 = T_{5-4}(m-4,n-4)+2,$ for any k, we have: $T_{5-4}(m,n) = T_{5-4}(m-k,n-k) = \frac{k}{2},$ for $m-k=2 \Rightarrow k=m-2,$ $T_(m,n) = T_{5-4}(2,n-m+2)+\frac{m}{2}-2.$ Based on first condition: $T_{5-4}(2,n-m+2) = C\binom{n-m+2}{2}\cdot 2^3 = \frac{(n-m+1)\cdot(n-m+1)}{2}\cdot 2^3$ $= 4\cdot(n-m+2)\cdot(n-m+1).$ $T_{5-4}(m,n) = 4\cdot(n-m+2)\cdot(n-m+1)+\frac{m}{2}-2$ $\approx 4\cdot(n-m+2)\cdot(n-m+1).$	
$T_5 = T_{5-1}+T_{5-2}+T_{5-3}+T_{5-4} = 4^{m-1}\cdot(n-m+2)\cdot(n-m+1)+4\cdot(n-m+2)\cdot(n-m+1)+m^4+4$ $\cdot(n-m+2)\cdot(n-m+1\approx 4^{m-1}\cdot(n-m+2)\cdot(n-m+1).$			1
$d = (d1*d4-d2*d3+d5*d6)/d7;$		$T_6 = const_6$	1

Based on Table 3, we have:

$$Total\_Cost = 1\cdot T_1 + Max(1\cdot T_2, 1\cdot T_3, 1\cdot T_4, 1\cdot T_5) + 1\cdot T_6$$

$$= 1\cdot Const_1 + Max(1\cdot n^3, 1\cdot n^3, 1\cdot n^3, 1\cdot 4^{m-1}\cdot(n-m+2)$$
$$\cdot(n-m+1)) + 1\cdot Const_6$$

.

Hence, the highest order is $4^{m-1}\cdot(n-m+2)\cdot(n-m+1)$. After eliminating constants and other lower grades, we can summarize the asymptotic time complexity as $O(2^2 m\cdot(n-m)^2)$.

The time complexity similarly can be concluded for each 9 cases.

Calculation of asymptotic time complexity of algorithm P 4, which is used to identify the pivot block with highest number of zero elements is presented on Table 4.

Table 4: Time complexity of Most_Zero_Elements_Block function

Function: *Most_Zero_Elements_Block*	**Cost**	**Time**
[m,n] = size(A);	$T_1 = const_1$	1
for $i = 1 : m$ for $j = 1 : n$ if $A(i, j) \sim= 0$ $B(i) = B(i) + 1$; $C(j) = C(j) + 1$;	$T_2(m,n) = m \cdot n$ Due to nested loop.	1
if $C(1)+C(2) < C(n-1)+C(n)$ $k = 1$;	$T_3 = const_3$	1
elseif $C(2)+C(n-1) < C(1)+C(n)$ $k = 2$;	$T_4 = const_4$	1
else $k = 3$;	$T_5 = const_5$	1
if $B(2)+B(m-1) < B(1)+B(m)$ $k = k+3$;	$T_6 = const_6$	1
elseif $B(1)+B(2) > B(m-1)+B(m)$ $k = k+6$;	$T_7 = const_7$	1

Based on Table 4, we have:

$$Total\_Cost = 1 \cdot T_1 + 1 \cdot T_2 + Max(1 \cdot T_3, 1 \cdot T_4, 1 \cdot T_5) + Max(1 \cdot T_6, 1 \cdot T_7) = 1 \cdot Const_1 + 1 \cdot m \cdot n + Max(1 \cdot Const_3, 1 \cdot Const_4, 1 \cdot Const_5) + Max(1 \cdot Const_6 + 1 \cdot Const_7).$$

After eliminating constants, we get the asymptotic time complexity of algorithm P 4 as $O(m \cdot n)$.

The analysis of the growth of time complexity graphically is presented on following graph for cases: number of columns from 50 to 54 and number of rows from 3 to 28.

As can be seen from Figure 1, the break point is on about half of number of columns.

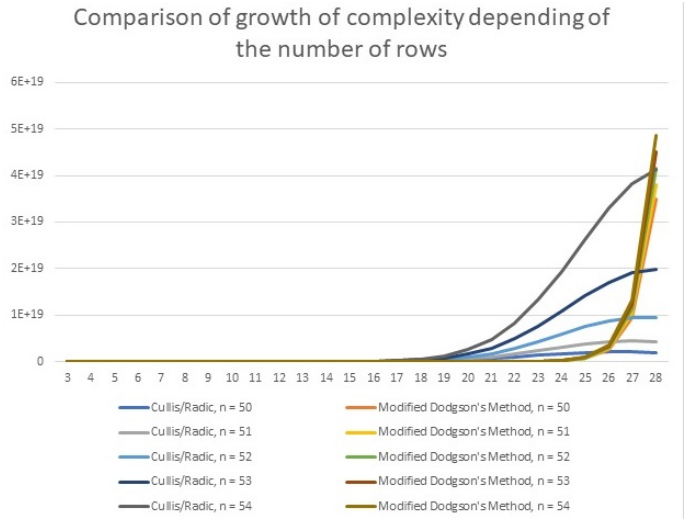


Figure 1: Comparison of growth of complexity depending on the number of rows, $50 \leq n \leq 54$, and $3 \leq m \leq 28$

Based on the analysis we can note that the Cullis/Radic definition (Algorithm P 1) is more efficient than the Dodgson's method (Algorithms P 2 and P 3) if the number of rows is higher than the half of number of columns, and in cases where the number of rows is lower or equal to half of number of columns, then the Dodgson's modified method is more efficient. Hence, we propose an algorithm which is a combination of both algorithms.

P 3: Modified algorithm (*det_Blocks*) based on theorem 2 (as example is considered case 1)

Step 1: Checking for conditions:

if $m = n$

Calculate square determinant with known methods.

else if $m = n - 1$

Transform determinant to square determinant, by adding one row with elements equal to 1.

$$d = det\_Ones(A);$$

else if $m < 3$ or $m = n/2$

Step 2: Identify all square determinants from the combination of columns:

Create loop from 1 to total number of combinations

$$D\{i\} = A(1 : m, B(i, 1 : m)));$$

Step 3: Calculate determinants of square blocks from D

Create Loop from 1 to total number of combinations

$$d = d + (-1)\hat{}(sum(1 : m) + sum(B(i, 1 : m))) * SquareDet(D\{i\});$$

else

Step 4: Calculate submatrices:

Calculate submatrices presented on theorem 1, calling *det_Comb* algorithm until the conditions of step 1 are met:

$$d1 = det\_Comb(A(1 : m-1, 1 : n-1));$$
$$d2 = det\_Comb(A(A(1 : m-1, 2 : n));$$

$$d3 = det\_Comb(A(2:m, 1:n-1));$$
$$d4 = det\_Comb(A(2:m, 2:n));$$
$$d5 = det\_Comb(A(2:m-1, 1:n));$$
$$d6 = det\_Comb(A(1:m, 2:n-1));$$
$$d7 = det\_Comb(A(2:m-1, 2:n-1));$$

Step 5: Calculate the result of the determinant as following:

$$d = (d1 * d4 - d2 * d3 + d5 * d6)/d7;$$

Step 6: Display the result of the determinant

Note: The algorithm P 5 can also be combined with algorithm P 3, with changes only in step 4, where in cases of several elements of original matrix equal to zero can be more efficient.

The worst-case time complexity of the above presented algorithm is where the number of rows is half the number of columns.

The asymptotic time complexity of the algorithm presented in P 5, is calculated in Table 5, where we have identified the worst-case and best-case time complexity as follows.

Table 5: Time complexity analysis of (det_Comb) function

Function: *det_Comb*	**Cost**		**Time**
$[m,n] = size(A);$	$T_1 = const_1$		1
if $m == n$ $d = det(A);$	$T_2 = n^3$		1
if $m == n-1$ $d = det\_Ones(A);$	Based on Algorithm 2.2 (See [11]), transforms determinant of order $(n-1)\times n$ to $n\times n$ by adding one row of elements equal to 1. Square determinant's time complexity is: $T_3 = O(n^3)$.		1
else if $m < 3$ $d = det\_A(A);$	As it is calculated the det_A time complexity is: $T_4(3,n) = C\binom{n}{3}\cdot 3^3 = \frac{n\cdot(n-1)\cdot(n-2)\cdot(n-3)!}{3!\cdot(n-3)!}\cdot 3^3 = n\cdot(n-1)\cdot(n-2)\cdot 4.5 \approx n^3.$		1
else if	$B = nchoosek(1:n, n/2);$	$T_5 = const_5$	1
	for $i = 1 : length(B)$ $d = d + (-1)^{\wedge}(sum(1:(n/2)) + sum(B(i,[1:(n/2)])))$ $*det((A([1:(n/2)], [B(i,[1:(n/2)])])));$	There are several methods to calculate square determinants with different time complexity, however we will be based on LU factorization method [16]: $T_6 = (\frac{n}{2})^3$	$C\binom{n}{n/2}$
else	$d1 = det\_Comb(A(1:n/2-1, 1:n-1));$ $d2 = det\_Comb(A(1:n/2-1, 2:n]));$ $d3 = det\_Comb(A(2:n/2, 1:n-1));$ $d4 = det\_Comb(A(2:n/2, 2:n]));$	$T_{7-1}(n/2,n) = 4\cdot T_{7-1}(n/2-1,n-1)+1,$ $T_{7-1}(n/2-1,n-1) = 4\cdot T_{7-1}(n/2-1-1,n-1-1)+1$ $= 4\cdot T_{7-1}(n/2-2,n-2)+1,$ $T_{7-1}(n/2,n) = 4\cdot(4\cdot T_{7-1}(n/2-2,n-2))+1+1$ $= 4^2\cdot T_{7-1}(n/2-2.n-2)+2,$ for any k, we have: $T_{7-1}(n/2,n) = 4^k\cdot T_{7-1}(n/2-k,n-k)+k,$ for $n/2-k = 2 \Rightarrow k = n/2-2,$ $T_{7-1}(n/2,n) = 4^{n/2-2}\cdot T_{7-1}(2,n-n/2+2)+n/2-2$ $= 4^{n/2-2}\cdot T_{7-1}(2,n/2+2)+n/2-2.$ Based on first condition: $T_{7-1}(2,n/2+2) = C\binom{n/2+2}{2}\cdot 2^3 = \frac{(n/2+2)\cdot(m/2+1)}{2}\cdot 2^3$ $= 4\cdot(n/2+2)\cdot(n/2+1).$ $T_{7-1}(n/2,n) = 4^{n/2-2}\cdot 4\cdot(n/2+2)\cdot(n/2+1)+n/2-2$ $\approx 4^{n/2-1}\cdot(n/2+2)\cdot(n/2+1).$	

	$d1 = det\_Comb(A(1:n/2-1,1:n-1));$ $d2 = det\_Comb(A(1:n/2-1,2:n]));$ $d3 = det\_Comb(A(2:n/2,1:n-1));$ $d4 = det\_Comb(A(2:n/2,2:n]));$	$T_{7-1}(n/2,n) = 4 \cdot T_{7-1}(n/2-1,n-1)+1,$ $T_{7-1}(n/2-1,n-1) = 4 \cdot T_{7-1}(n/2-1-1,n-1-1)+1$ $= 4 \cdot T_{7-1}(n/2-2,n-2)+1,$ $T_{7-1}(n/2,n) = 4 \cdot (4 \cdot T_{7-1}(n/2-2,n-2))+1+1$ $= 4^2 \cdot T_{7-1}(n/2-2.n-2)+2,$ for any k, we have: $T_{7-1}(n/2,n) = 4^k \cdot T_{7-1}(n/2-k,n-k)+k,$ for $n/2-k = 2 \Rightarrow k = n/2-2,$ $T_{7-1}(n/2,n) = 4^{n/2-2} \cdot T_{7-1}(2,n-n/2+2)+n/2-2$ $= 4^{n/2-2} \cdot T_{7-1}(2,n/2+2)+n/2-2.$ Based on first condition: $T_{7-1}(2,n/2+2) = C\binom{n/2+2}{2} \cdot 2^3 = \frac{(n/2+2)\cdot(m/2+1)}{2} \cdot 2^3$ $= 4 \cdot (n/2+2) \cdot (n/2+1).$ $T_{7-1}(n/2,n) = 4^{n/2-2} \cdot 4 \cdot (n/2+2) \cdot (n/2+1)+n/2-2$ $\approx 4^{n/2-1} \cdot (n/2+2) \cdot (n/2+1).$	
	$d5 = det\_Comb(A(2:n/2-1,1:n));$	$T_{7-2}(n/2,n) = T_{7-2}(n/2-1,n)+1,$ $T_{7-2}(n/2-1,n) = T_{7-2}(n/2-1-1,n)+1 = T_{7-2}n/2-2,n)+1,$ $T_{7-2}(n/2,n) = T_{7-2}(n/2-2,n)+1+1 = T_{7-2}(n/2-2,n)+2,$ for any k, we have: $T_{7-2}(n/2,n) = t_{7-2}(2,n/2-2)+n/2-2.$ Based on first condition: $T_{7-2}(2,n/2-2) = C\binom{n/2-2}{2} \cdot 2^3 = \frac{(n/2-2)\cdot(n/2-3)}{2} \cdot 2^3$ $= 4 \cdot (n/2-2) \cdot (n/2-3).$ $T_{7-2}(n/2,n) = 4 \cdot (n/2-2) \cdot (n/2-3)+n/2-2$ $\approx 4 \cdot (n/2-2) \cdot (n/2-3).$	
	$d6 = det\_Comb(A(1:n/2,2:n-1));$	$T_{7-3}(n/2,n) = T_{7-3}(n/2,n-1)+1,$ $T_{7-3}(n/2,n-1) = T_{7-3}(n/2,n-1-1)+1 = T_{7-3}(n/2,n-2)+1,$ $T_{7-3}(n/2,n) = T_{7-3}(n/2,n-2+1+1 = T_{7-3}(n/2,n-2)+2,$ for any k, we have: $T_{7-3}(n/2,n) = T_{7-3}(n/2,n-k)+k,$ for $n-k = n/2+1 \Rightarrow k = n-n/2-1 = n/2-1,$ $T_{7-3}(n/2,n) = T_{7-3}(n/2,n-n/2+1)+n/2-1$ $= T_{7-3}(n/2,n/2+1)+n/2-1.$ Based on first condition: $T_{7-3}(n/2,n/2+1) = C\binom{n/2+1}{n/2} \cdot (n/2)^3 = (n/2+1) \cdot (n/2)^3$ $= (n/2)^4+(n/2)^3.$ $T_{7-3}(n/2,n) = (n/2)^4+(n/3)^3+n/2-1 \approx (n/2)^4.$	
	$d7 = det\_Comb(A(2:n/2-1,2:n-1));$	$T_{7-4}(n/2,n) = T_{7-4}(n/2-2,n-2)+1,$ $T_{7-4}(n/2-2,n-2) = T_{7-4}(n/2-2-2,n-2-2)+1$ $= T_{7-4}(n/2-4,n-4)+1,$ $T_{7-4}(n/2,n) = T_{7-4}(n/2-4,n-4)+2,$ for any k, we have: $T_{7-4}(n/2,n) = T_{7-4}(n/2-k,n-k)+k/2,$ for $n/2-k = 2 \Rightarrow k = n/2-2,$ $T_{7-4}(n/2,n) = T_{7-4}(2,n/2+2)n/4-2.$ Based on first condition: $T_{7-4}(2,n/2+2) = C\binom{n/2+2}{2} \cdot 2^3 = \frac{(n/2+2)\cdot(n/2+1)}{2} \cdot 2^3$ $= 4 \cdot (n/2+2) \cdot (n/2+2).$ $T_{7-4}(n/2,n) = 4 \cdot (n/2+2) \cdot (n/2+1)+n/4-2$ $\approx 4 \cdot (n/2+2) \cdot (n/2+1).$	
$T_7 = T_{7-1}+T_{7-2}+T_{7-3}+T_{7-4} = 4^{n/2-1} \cdot (n/2+2) \cdot (n/2+1)+$ $4 \cdot (n/2-2) \cdot (n/2-3)+(n/2)^4+4 \cdot (n/2+2) \cdot (n/2+1) \approx 4^{n/2-1} \cdot (n/2+2) \cdot (n/2+1).$			1
$d = (d1*d4-d2*d3+d5*d6)/d7;$	$T_8 = const_8$		1

Based on Table 5, we have:

$$Total\_Cost = 1 \cdot T_1 + Max(1 \cdot T_2, 1 \cdot T_3, 1 \cdot T_4, 1 \cdot T_5, C\binom{n}{n/2}$$

$$\cdot T_6, 1 \cdot T_7) + 1 \cdot T_8 = 1 \cdot Const_1 + Max(1 \cdot n^3, 1 \cdot n^3, 1 \cdot n^3,$$

$$1 \cdot Const_5 + C\binom{n}{n/2} \cdot (\frac{n}{2})^3, 1 \cdot 4^{n/2-1} \cdot (n/2+2) \cdot (n/2+1)) + 1)$$

$$+1 \cdot Const_8$$

.

Hence, the highest order is $C\binom{n}{n/2} \cdot (\frac{n}{2})^3$. After eliminating constants and other lower grades, we can summarize the worst-case asymptotic time complexity as $O(\frac{n!}{((n/2)!)^2} \cdot (n/2)^3)$.

While the best-case is $O(n^3)$, for $m = 3$, calculated as follows:

For Cullis/Radic we have:

$$Total\_Cost = 1 \cdot T_1 + 1 \cdot T_2 + 1 \cdot T_3 + Max(1 \cdot T_4, C\binom{n}{n/2} \cdot T_5)$$

$$= 1 \cdot Const_1 + 1 \cdot Const_2 + 1 \cdot Const_3 + Max(1 \cdot n^3, C\binom{n}{3} \cdot 3^3)$$

.

While,

$$Max(1 \cdot n^3, C\binom{n}{3} \cdot 3^3) = Max(1 \cdot n^3, \frac{n!}{3! \cdot (n-3)!} \cdot 3^3)$$

$$= Max(1 \cdot n^3, \frac{n \cdot (n-1) \cdot (n-2) \cdot (n-3)!}{3! \cdot (n-3)!} \cdot 3^3)$$

Since the n^3 is the highest order, the asymptotic time complexity is $O(n^3)$.

For generalized/modifed Dodgson's method, we have:

$$Total\_Cost = 1 \cdot T_1 + Max(1 \cdot T_2, 1 \cdot T_3, 1 \cdot T_4, 1 \cdot T_5) + 1 \cdot T_6$$

$$= 1 \cdot Const_1 + Max(1 \cdot n^3, 1 \cdot n^3, 1 \cdot n^3, 1 \cdot 4^{3-1} \cdot (n-3+2)$$

$$\cdot (n-3+1)) + 1 \cdot Const_6$$

.

Also, in this case since the n^3 is the highest order, the asymptotic time complexity is $O(n^3)$.

3 Conclusions

In this paper we have analyzed the asymptotic time complexity of algorithms based on Cullis/Radic definition and generalized/modified Dodgson's Condensation method/s for rectangular determinant calculations. From the calculations we noted that the asymptotic time complexity for Cullis/Radic definition is $O(C\binom{n}{m} \cdot m^3)$, while for the generalized/modified Dodgson's Condensation method/s the asymptotic time complexity is $O(2^2 m \cdot (n-m)^2)$.

Further we have analyzed which complexity grows faster and tested for rectangular determinant of order for $50 \leq n \leq 54$, and $3 \leq m \leq 28$, and from analysis it is noted that the break point is on about half of number of columns compared to number of rows. In cases where the number of columns is less than the half of the number of rows, then the Dodgson's Condensation method/s are growing slower than the Cullis/Radic definition, otherwise the Cullis/Radic definition is growing slower. From this analysis we have proposed a combined algorithm where it calculates determinants with Cullis/Radic definition in cases where the number of columns is higher than the half of number of rows and calculates determinants with Dodgson's Condensation method/s in cases where the number of columns is lower than the half of number of rows.

From where we calculated the worst-case asymptotic time complexity as $O(\frac{n!}{((n/2)!)^2} \cdot (n/2)^3)$, while the best-case asymptotic time complexity is when the $m = 3$, and it is calculated as $O(n^3)$.

References

[1] A. Amiri, M. Fathy, and M. Bayat. "Generalization of Some Determinantial Identities for Non-Square Matrices Based on Radic's Definition." *TWMS Journal of Pure and Applied Mathematics*, 1(2):163-175, 2010.

[2] M. Bayat, "A Bijective Proof of Generalized Cauchy–Binet, Laplace, Sylvester and Dodgson Formulas." *Linear and Multilinear Algebra*, 2020.

[3] T. H. Cormen, C. E. Leiserson, R. L. Rivest, R. L., and C. Stein, *Introduction to Algorithms 4th Edition*. The MIT Press Cambridge, Massachuestts London, England, 2022.

[4] C. E. Cullis, *Matrices and Determinoids*. Cambridge: University Press, 1913.

[5] A. Makarewicz and P. Pikuta, "Cullis–Radic Determinant of a Rectangular Matrix Which Has a Number of Identical Columns." *Annales Universitatis Mariae Curie-Sklodowska*, 74(2):41-60, 2020.

[6] A. Makarewicz, P. Pikuta, and D. Szalkowski, "Properties of the Ddeterminant of a Rectangular Matrix." *Annales Universitatis Mariae Curie-Sklodowska*, 68(1):31-41, 2014.

[7] R. E. Neaplitan, *Foundations of Algorithms*. Cambridge: Jones and Bartlett Learning, 2015.

[8] M. Radic, "Definition of Determinant of Rectangular Matrix." *Glasnik Matematicki*, pp. 17-22, 1966.

[9] K. H. Rosen, *Discrete Mathematics and Its Applications 8th Edition*. New York: McGraw-Hill Education, 2019.

[10] A. Salihu, H. Snopce, J. Ajdari, and A. Luma, "Generalization of Dodgson's Condensation Method for Calculating Determinant of Rectangular Matrices." *2nd IEEE International Conference on Electrical, Computer and Energy Technologies (ICECET)*, Prague, 2022.

[11] A. Salihu and F. Marevci, ”Chio’s-like Method for Calculating the Rectangular (Non-Square) Determinants: Computer Algorithm Interpretation and Comparison.” *European Journal of Pure and Applied Mathematics*, 14(2):431-450, 2021.

[12] S. S. Skiena, *The Algorithm Design Manual*. London: Springer-Verlag London Limited, 2008.

[13] P. Stanimirovic and M. Stankovic, ”Determinants of Rectangular Matrices and the Moore-Penrose Inverse.” *Novi Sad J Math.*, 27(1):53-69, 1997.

[14] M. Stojakovic, ”Determinante Nekvadratnih Matrica.” *Vesnik DMNRS*, 1952.

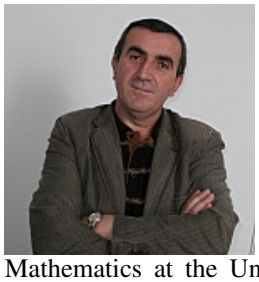
[15] A. P. Sudhir, ”Generalisations of the Determinant to Interdimensional Transformations: A Review.” *arXiv:1904.08097v1*, 2019

[16] W. Xingbo and X. Yaoqi, ”How Difficult To Compute Coefficients of Characteristic Polynomial?” *International Journal of Research Studies in Computer Science and Engineering (IJRSCSE),*, 3(1):7-12, 2016.

Armend Salihu is a PhD Candidate at the South East European University, Faculty of Contemporary Sciences. In 2009 he has received bachelor degree at the University of Prishtina, Faculty of Electrical and Computer Engineering, while in 2017 he received master degree in the field of computer Science from the University for Business and Technology, Faculty of Computer Sciences and Engineering. Currently he is engaged as teaching assistant at the University of Prishtina, Faculty of Mathematics and Natural Sciences.

Halil Snopce is a full professor at the South East European University. He has been graduated in Mathematics in 1997 at the University of ”St. Cyril and Methodius”, Faculty of Natural and Mathematical Sciences. In 2007 he received master degree in Mathematics at the University of Tirana, Faculty of Natural and Mathematical Sciences, with the main topics in numerical analysis. In 2011 he has received his PhD in Computer Science and Applied Mathematics in the CST-Faculty at the South East European University. His speciality is parallel processing.

Artan Luma is a full professor at the South East European University. He has been graduated as Engineer of Informatics in Computer Science at the State University of Tetovo in 1997. He received Master of Electrical Engineering Science at the University of Prishtina, Faculty of Electrical and Computer Engineering in 2007. In 2011 he received PhD in Computer Science at the South East European University, Faculty of Contemporary Sciences and Technologies. His speciality is cryptography.



Jaumin Ajdari is a full professor at the South East European University. He has been graduated as Engineer in Applied Mathematics, as well as Master in Mathematics at the University of Zagreb, Faculty of Natural Science and Mathematics. He also received Master of Science in Mathematics at the University of Tirana, Faculty of Natural Sciences, Department of Numerical Mathematic and Parallel processing in 2006. In 2011 he has received his PhD in Mathematical Sciences at the University of Tirana, Faculty of Natural Sciences. His speciality is parallel processing.

Comparative Study Between Aura and Clique Blockchain-Based Proof of Authority Algorithms on Wireless Sensor Network

Delphi Hanggoro*, Jauzak Hussaini Windiatmaja*, Riri Fitri Sari *
Universitas Indonesia, Depok 16424, INDONESIA

Abstract

Using blockchain in Wireless Sensor Network (WSN) has solved the problems of centralized authority, heterogeneity, authentication, and security. However, no blockchain consensus is intended for WSN applications. Usually, permissioned blockchain is used to integrate into the WSN because of its fast transaction time and easy management member. This study compared two permissioned blockchains consensuses Proof-of-Authority algorithms named Aura and Clique to determine which algorithm is more appropriate for WSN. We compare the suitability of Aura and Clique algorithms, how they work on WSN topology and evaluate each algorithm's transaction speed and block drop. The result shows the transaction speed of Aura has a transaction time of 31.62ms, slower than Clique, which only requires 6.03ms for 100 transactions. Aura has no dropped blocks, whereas Clique has approximately 8 dropped blocks in the number of transactions. This happens because the Clique algorithm has a GHOST protocol that only stores the blocks proposed by one Leader. Aura has a longer transaction time, but Aura does not have discarded blocks. All data from WSN can enter the network. Thus, Aura is more suitable than Clique to apply to WSN.

Key Words: Wireless Sensor Network, blockchain, proof-of-authority, aura, clique.

1 Introduction

Blockchain technology is known as a secure distributed database. Other technologies needed the security advantage of blockchain, such as the Internet of Things (IoT) and Wireless Sensor Network (WSN). Yet, blockchain application to IoT and WSN has solved several problems, including centralized authority, heterogeneity, authentication, and security.

Some of the key challenges of blockchain integration on WSN are resource constraints and network architecture. To overcome resource problems, previous studies modified the consensus of existing public blockchains such as Proof-of-Work (PoW) [21] and Proof of Stake (PoS) [7] to reduce power and memory use on the sensor devices.

*delphi.hanggoro@ui.ac.id, jauzak.hussaini@ui.ac.id; riri@ui.ac.id

However, lately there are some new types of blockchain, such as private and consortium, which are intended for devices that have limited resources. The private type is more for personal use in a company, while consortium (permissioned) is more commonly used in several companies with the same business interest. According to Biswas et al. [5], permissioned blockchain is a type of blockchain that is intended for a business of two or more companies, network members can also be easily maintained. In addition, the permissioned blockchain does not consume enormous resources and has fast transaction times, which is suitable for IoT integration. Singh et al. [25] study reinforce the use of a permissioned blockchain, proved that the Proof-of-Authority (PoA) [24] consensus can be a lightweight solution for IoT smart homes.

Proof-of-Authority (PoA) is part of a permissioned blockchain developed and deployed on the Ethereum private network. The way Proof of Authority (PoA) works is by leveraging identity values, so block validators are not risking coins, but their own reputation. Therefore, the PoA blockchain is secured by an arbitrarily selected validation node as a trustworthy entity. Proof of Authority relies (PoA) on several block validators. This makes it a highly scalable system. Pre-approved participants who act as system moderators verify blocks and transactions. Networks that use PoA consensus do not require any mining activity. This type of consensus mechanism also does not require a lot of resources, so it is appropriate to be integrated into the WSN.

Furthermore, to answer the challenges of network architecture Alghamdi et al. [1] tried the solution of Bozorgi et al. [6] and Zhang et al. [29] to use the clustered network architecture on the WSN network which is assumed to be hierarchical routing algorithms as a solution for implementing blockchain on the WSN. The results of research by Alghamdi et al. [1] shows lower energy consumption than flat routing algorithm on large-scale WSN and have greater adaptability. In addition, Cui et al. [10] has also implemented clustered WSN in his research. Based on his research, clustered WSN has flexibility in the division of tasks so that each device has a specific task that does not burden other devices.

In Ethereum there are two different algorithms for PoA: Aura [2] and Clique [9], which have differences in the validation process and the number of block proposers (Leaders).

This study analyses the Aura and Clique algorithm's compatibility with WSN and evaluates the performance. Our contribution to this research is to compare the suitability of the Aura and Clique's works on WSN topology. Subsequently, we evaluate and compare the transaction speed and block drop on the Aura and Clique algorithm.

The rest of this research is structured as follows: Section 2 is the literature review of blockchain and consensuses, blockchain integration on IoT, and PoA details. Section 3 discusses the comparison method. Section 4 presents the results and discussions. Finally, Section 5 describes the conclusions.

2 Literature Review

2.1 Blockchain and Consensus Algorithm.

Blockchain is a distributed and decentralized data structure. Primarily, blockchain is used to record a digital transaction on a crypto network. "Bitcoin" [21] is the original application of the use of blockchain for digital currency which was developed by Satoshi Nakamoto in 2008. Bitcoin is formed by a Peer-to-Peer (P2P) network. Bitcoin does not require a central server to host the blockchain and store transaction history, unlike server-based systems. In contrast, bitcoin keeps a copy of the blockchain/ledger on all network members, thus forming a decentralized public ledger.

Each block consists of data that has been verified and then wrapped by a hash with a specific target. The block is linked to the previous block's hash, as shown in Figure 1. Once a block is created, it will be distributed to all nodes on the blockchain to form a decentralized blockchain.

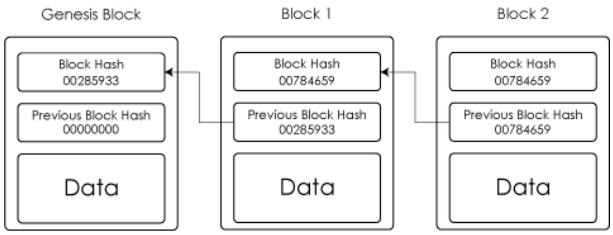


Figure 1: Blockchain recording mechanism

Blockchain security is made up of four technological features that ensure reliable and secure data services [28]:

(1) Distributed ledger: all network members share the same data, making tamper or change difficult. All members are responsible for monitoring legitimate transactions. (2) Authorization and asymmetric encryption: although every member can see data that has entered the network, every identity is properly encrypted and can only be accessed by the data owner, who can ensure identity privacy. (3) Smart contracts: are predefined codes that are trusted and tamper-proof; smart contracts will be executed automatically when certain conditions are met. (4) Consensus Algorithm: a key feature of blockchain, a consensus algorithm is a mechanism for all nodes on a blockchain network to agree on the data that will enter the network.

The consensus used in a blockchain system depends on the type of blockchain. There are three types of blockchain: Public, Private and Consortium.

2.1.1 Public Blockchain. Public blockchain is the first type that exists on the blockchain. Each member on the network has the same power to read and write data on the blockchain network with agreed rules. Each member can freely enter and leave the network, validating transactions with the required hardware and certain software. Thus, a public blockchain is a type of blockchain that is fully distributed and decentralized because there is no entity that manages and controls the rules of the blockchain network.

However, due to the large number of devices, public blockchain generally requires a large amount of time and resources to reach an agreement. Examples of popular consensus of this type are: Proof-of-Works (PoW) used by bitcoin and Proof-of-Stake (PoS) used by Ethereum.

Proof-of-Work (PoW) [21] PoW works with the concept of "mining" competition. Each node that wants to get a reward must compete simultaneously to solve a mathematical puzzle of a certain hash target. The node that solves the puzzle first will be rewarded with the cryptocurrency or token used in the system, for example, Bitcoin or Ether on Ethereum. PoW is a well-known consensus with excellent integrity and can tolerate several attacks [11]. However, PoW has some drawbacks, such as consuming many resources, such as computing and electrical power. Such waste causes many problems to be integrated into other fields with limited resources.

Proof-of-Stake (PoS) [7] Proof-of-Stake (PoS) is a development of PoW that consumes a lot of resources. The mining concept on PoW is still carried out on PoS, but there is no competition in PoS. PoS will select nodes that can propose blocks based on the number of stakes or cryptocurrencies on the network to replace the competition. The node with the highest stake will be chosen as the miner. Working concepts like this can drastically solve the problem of resource usage in PoW. However, with the work concept based on "stake", an additional problem arises: it will enrich nodes that already have a lot of stakes. Meanwhile, nodes with few stakes can not become block proposers, so the distribution of energy use is uneven. In addition, multiple nodes with the highest stake can dominate the network and increase the risk of a 51 percent attack.

2.1.2 Private Blockchain. Private blockchains have a different structure from public blockchains, while public blockchains are fully decentralized, private blockchains have a fully centralized structure. To be able to enter the blockchain network, new members need permission from the centralized entity to be able to access, write and validate blocks on the blockchain. The advantage of a private blockchain is that it provides privacy to all members of the blockchain network compared to public blockchains. However, it has drawbacks because there are several parties who have full control over the

rules of the blockchain network.

Private blockchains are suitable for cases where readability or public audit is not required. In addition, a high level of trust must be built between participants. Compared to public blockchains, private blockchains have faster transaction speeds and lower transaction costs because in general the mathematical competition process will be replaced by a verification process by each member. "Raft" [22] is a consensus example of implementing a private blockchain.

Raft [22] Raft is an implementation of ordering service consensus, which is a development of Crash Fault Tolerant (CFT). CFT allows a consensus process to continue to run even though the process has N failures, while there are N/2+1 nodes running. In addition, Raft implements a "Leaders and Followers" process that uses consenters on the ordering service nodes. Raft's most popular application is the Hyperledger Fabric. In Hyperledger Fabric, Raft is implemented as a bridge link to build PBFT consensus, because PBFT and Raft have similar procedures in Hyperledger Fabric integration.

2.1.3 Permission Blockchain. Consortium blockchain (permissioned blockchain) is a combination of public and private blockchain. Permissioned blockchains have the characteristics of being partly decentralized, only some members of the network have rights to access and validate transactions. Rights on the network are determined by the identity and role of the members in the system's design. Usually, a permissioned blockchain comprises several companies with the same business interests, so it requires a smart contract to perform and validate identities and business logic before committing to transactions.

Popular permissioned blockchain implementations are Hyperledger with consensus Practical Byzantine Fault Tolerance (PBFT) and Proof-of-Elapsed-Time (PoET), OpenEthereum with consensus Authority Round (AuRa), Go-Ethereum with consensus Clique.

Proof-of-Elapsed-Time (PoET) [11] PoET is a type of permissioned blockchain developed by Intel in early 2016. Consensus PoET uses the lottery concept for each network member, which requires members to wait for some time according to the lottery they receive. If one of the members has finished proposing a block, the time to be waited for will be reset and get a random time again. Thus each member has the same opportunity to be able to propose a block. The most famous application of PoET is on the Hyperledger Sawtooth platform.

Practical Byzantine Fault Tolerance (PBFT) [8] Consensus that use rotation to select proposers (Leader) of blocks on the blockchain network. In PBFT, one Leader will be chosen while the others will be the backup. Each node must be connected to the other. The validation process in PBFT requires all nodes to check each other's contents of blocks that the Leader has proposed, so that the more network members, the longer the validation time.

Proof-of-Authority (PoA) [12] Like PBFT, PoA adopts a round-robin rotation of proposers (Leader) so that all nodes will get a turn to become block proposers. Proof of Authority (PoA) is a family of consensus algorithms for permissioned blockchains known for their improved performance compared to Byzantine Fault Tolerance algorithms. PoA was initially proposed as part of the Ethereum ecosystem for private networks.

2.2 Blockchain Integration on IoT and WSN

Implementing blockchain technology was first introduced by Satoshi Nakamoto [21] in 2008 for cryptocurrencies, and advanced to implementing finance, healthcare, decentralized applications, voting systems and the Internet of Things (IoT) [4, 13, 15, 18, 26]. Blockchain has the characteristics of decentralization, immutable, integrity and reliable. With these characteristics, blockchain can solve some of the existing IoT issues. Several studies on blockchain implementation in IoT have solved issues such as centralized authority, heterogeneity and authentication [3, 5, 14, 16, 19, 20, 27].

According to Biswas et al. [5], the use of permissioned blockchain is more appropriate than public blockchain because permissioned blockchain has a less consumption of computing power, energy and storage resources than public blockchain. In their study, Biswas et al. [3] built a secure framework for IoT using Hyperledger Fabric. They designed each IoT device to implement a client peer and become part of the blockchain network. Besides that, they also grouped some IoT devices and used one of them to become a single peer global. As a result, they can significantly increase the speed of transactions in the blockchain network.

Ayoade et al. [3] have built a decentralized data management system on top of Ethereum that uses smart contracts to manage access permissions and audit trails. It can record all data on the blockchain. As a result, Ethereum's transaction throughput per second will increase as the write workload increases, limiting the blockchain's scalability. Thus, they suggest using a permissioned blockchain to save time, as all nodes are assumed to know each other. Singh et al. [25] has also tested the use of a permissioned blockchain. They have tested the performance of the consensus PoA algorithm and compared it to consensus PoW for smart home device management with the raspberry pi 3. As a result, PoA uses much lower CPU utilization compared to PoW. Thus, PoA has the potential to be a lightweight consensus solution for IoT.

Aside from resource consumption, blockchain and WSN have problems with the way they communicate. WSN communicates on a multi-hop, while blockchain uses peer-to-peer communication. To resolve the differences in how to communicate on IoT and blockchain, several researchers apply clustering to the WSN network on blockchain. Clustering is a method in the form of groups on WSN nodes. Each cluster has a common node, a cluster head and a base station. The cluster head collects data from ordinary nodes and then collects it at the base station. Clustering on WSN has been shown to consume less energy and has better adaptation than flat routing algorithms [6, 29].

Cui et al. [10] use blockchain as identity authentication on WSN, usually relying on trusted third parties with a single point of failure risk. They divide the entire network into several types based on the capabilities of the nodes, namely ordinary nodes, base stations and cluster heads that form a hierarchical network. They divided the blockchain network into public and local network. Each base station and end-user are interconnected, forming a public blockchain. Public blockchains are useful for registering and authenticating cluster node heads and providing authenticated communication between nodes across WSNs. The local blockchain registers ordinary nodes for authentication. Ordinary nodes create smart contracts deployed to the cluster head to verify registration and authentication requests. The security and performance analysis shows that the scheme has comprehensive security and better performance.

2.3 Proof-of-Authority

In its implementation, Aura and Clique have different validation methods. Both algorithms have the same first stage where the block proposer (Leader) is currently proposing a new block (block proposal). However, the Aura algorithm requires a second stage, namely block acceptance, while the Clique algorithm does not, as we can see in Figure 2.

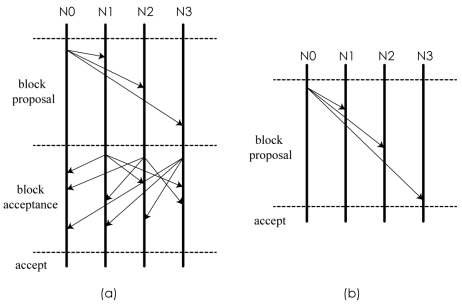


Figure 2: Step-by-step message exchange at the proof-of-authority algorithm. (a) Aura, (b) Clique

2.3.1 Authority Round (AuRa). The AuRa algorithm was first used by an Ethereum client named OpenEthereum [23] which uses the Rust programming language. All members on Aura are assumed to be synchronized in UNIX time t in a synchronous network.

$$\frac{UNIX\,time}{t} \tag{1}$$

Time is divided into discrete steps of duration t, determined by the equation 1. Each authority calculates deterministically the index i of each step as

$$i = t/StepDuration \tag{2}$$

Where $StepDuration$ is a constant that determines time UNIX for each step. The Leader in step i is the authority identified by equation 3, where N = number of nodes.

$$l = i \bmod N \tag{3}$$

Each authority has a local transaction queue (Qtx) and blocks queue (Qb). Every transaction that has been made will be collected at $(Qtxn)$ for each authority. At each step, the Leader enters the transactions in $(Qtxn)$ into block b and then broadcasts the block to another authority (block proposal step in Figure 2(a)). Then each authority will send the received blocks to other authorities for validation (acceptance block step in Figure 2(b)). If all authorities validate that block b received is the same, then block b will enter the queue (Qb). All blocks that are validated even if they are empty will enter the queue, but if the block to be included in the queue is proposed by an authority that is not expected to become a Leader then the block will be rejected.

Block b in queue Qb will be committed to the blockchain network when most authorities have proposed their block. In these networks, the majority of authorities can be trusted, which can prevent suspicious leaders from committing illegal blocks. Any suspicious behavior (such as different block contents in the validation process) will trigger a vote in which a majority can reliably blacklist the current Leader. The blocks they propose can be discarded before being executed and committed on the blockchain network.

Block finality in the Aura algorithm is a condition where the block in the Qb queue will enter the network when the queue has reached a certain condition. In step s1 on the blockchain, the block is committed up to two times, while the block $bi+1 \cdots bi+n$ is pending. Block bi can be committed because $n = \frac{k}{2}+1$ where k is the number of proposed blocks. The next block has been proposed after bi, and thus block bi can be finalized. Likewise, in step $s2$, block $bi+1$ can be finalized because the queue contains further blocks, as shown at Figure 3.

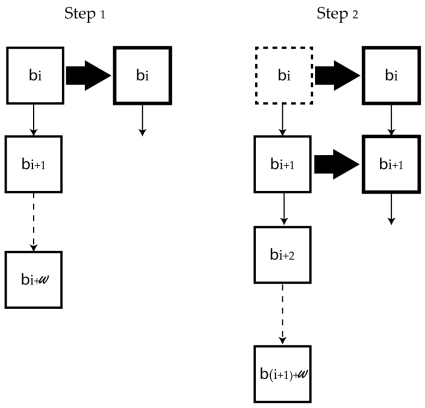
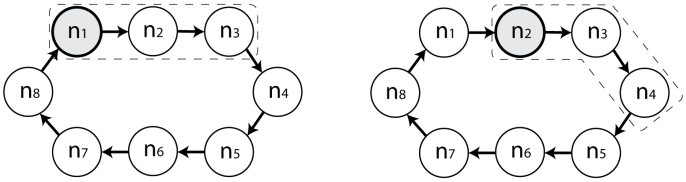


Figure 3: Aura finality mechanism

2.3.2 Clique. The Clique algorithm [9] is the original consensus used on the Go-Ethereum (Geth) platform [17]. In Clique's algorithm a member of the network is named "authority" which has a unique ID. Each authority is responsible for validating and mining blocks (block proposer) on the blockchain network. The task of becoming a block proposer is then determined using round robin fashion on the registered

unique ID.

The Clique algorithm determines the steps and the Leader by combining the amount of authority and the block number. In the Clique algorithm, n authorities may propose blocks at each step, as shown in Figure 4 (a), $n1$ being the Leader, $n2$ and $n3$ can propose blocks. To avoid an authority that can screw up the network, each authority is only allowed to propose one block every $N/2+1$ block. So, there are at least $N(N/2+1)$ authorities allowed to propose blocks for each step. Just like Aura, if the Leader acts suspiciously, we can expel them. Voting against other authorities can be carried out at every step, and if conditions are met, the authority is removed from the list of valid authorities.



(a) (b)

Figure 4: Clique leader selection

Figure 4 shows two successive Leader selection steps. For example, if there are $N=8$ authorities on the network, then there are $N(N/2+1)=3$ authorities who have the right to propose blocks at every step. So, as we can see in Figure 3(a), $n1$ is the current Leader, while $n2$ and $n3$ may propose blocks. In Figure 3(b), $n1$ cannot submit a block because it is no longer a Leader which requires it to wait for a number of $N/2+1$ steps to propose another block. Meanwhile, $n4$ is the sub-leader who can propose blocks, and $n2$ is the current Leader.

Because multiple Leaders can propose blocks during each step, forks can occur. However, the possibility of a fork is limited because every non-leading authority that proposes a block delays its block randomly, so the Leader's block will probably be the first to be accepted by all authorities. If a fork occurs, the GHOST protocol [12] is used. GHOST (Greedy Heaviest Observed Subtree) protocol is a protocol on the blockchain. This protocol is tasked with selecting a valid chain and proceeding as the main chain.

In the Clique algorithm, the GHOST protocol used is based on a block score approach, i.e., the leader block with the higher score will be the block that enters the blockchain, thus ensuring that the fork will eventually be resolved.

Fork in Clique algorithm is a condition where the last block at each node is different, so the network must determine which block will be used as a reference and the main chain. Figure 5 (left). illustrates the step in which authority leader $n2$ and authority non-leader $n3$ propose a new block simultaneously. In this step, $n3$ and $n4$ have the second block (b2) proposed by $n3$. Whereas $n1$, $n2$ and $n5$ have blocks proposed by $n2$. In the end, the block proposed by $n3$ on $n4$ will be replaced by $n2$. As shown in Figure 4 (right), each authority easily detected the resulting fork during the next block because the proposed next block will reference the previous block that is not available for the authority. The GHOST protocol used in the Clique algorithm is a scoring mechanism where if there are two authorities who propose a block simultaneously, only the block from the Current Leader $(n2)$ will enter the blockchain. Therefore, the GHOST protocol can overcome the fork.

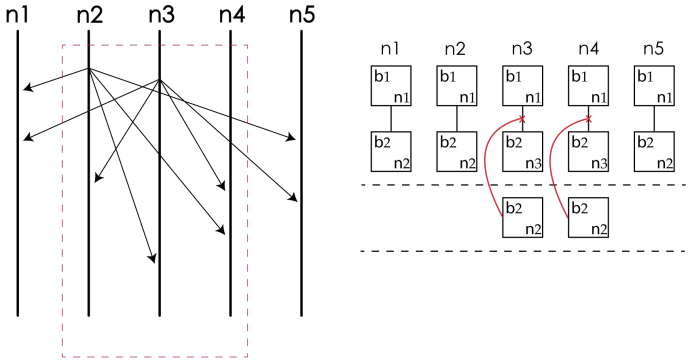


Figure 5: GHOST protocol mechanism when fork occurred

3 Comparison Method

In this study, two aspects will be compared and analyzed. First, we describe the experimental setup on Aura and Clique to compare transaction time and block drop performance. Second, we explain the method of comparing the message exchange of the Aura and the Clique algorithms on WSN with the cluster topology.

3.1 Experiment Setup

We carried this performance comparison experiment with Virtual Machine software with six processor cores and 8 Gb of memory on a personal laptop with Intel I7-9750H, 32 GB DDR4 memory, Nvidia GTX 1660 Ti, and 1 Tb M.2 NVME SSD. We are testing Aura on Ethereum Client OpenEthereum version 3.3.2 and Clique on Ethereum Client GoEthereum (GETH) version 1.10.14.

Table 1 contains the configurations listed in the test. The number of nodes and authority used is 8, the block interval is 15 seconds and the total transactions made are 100 per node. The default difficulty used is 1. To simulate IoT conditions, each node will send one transaction every 5 seconds.

3.1.1 Message exchange Mechanism. Based on the message exchange mechanism in Aura and Clique, the exchange of proposal block messages will be distributed to each network node and accepted by each node. The key challenge of implementing Proof-of-Authority on WSN is the different ways of communication. Blockchain communicates peer-to-peer, while WSN communicates in a multi-hop manner with a mesh topology. Figure 6 shows an example of implementing

Table 1 : Simulation configuration settings

Parameter	Authority Round	Clique
Number of Node	8	8
Number of Authorities	8	8
Block interval	15s	15s
Total transaction	100 per node	100 per node
Difficulty	1	1

the Proof-of-Authority (PoA) message exchange in a mesh topology commonly used in WSN networks.

When Proof-of-Authority is applied directly to the mesh topology, as shown in Figure 6, each transaction will consume a large amount of energy on the network. For example, when node 1 wants to submit a message for a block proposal, node 1 must deliver the message to node 2 through node 8. However, node 1 cannot communicate to node 8 directly, so the message must be delivered in a multi-hop through node 2 – node 4 – node 7 or another path to node 8. Naturally, the intermediary device (node 2, node 4 and node 7) will have more burden to convey messages from other nodes, so it is necessary to choose the right topology to implement Proof-of-Authority on WSN.

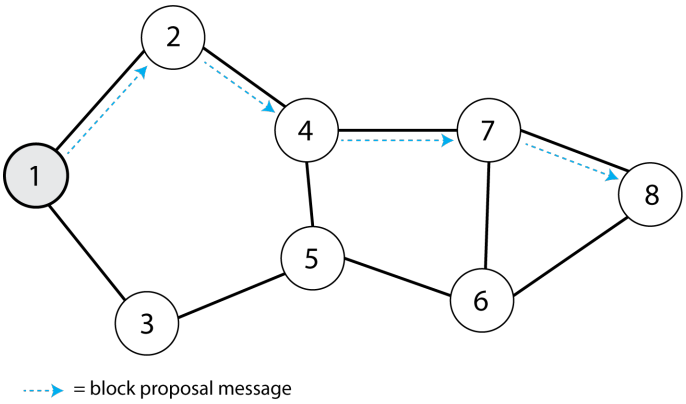


Figure 6: PoA message exchange on mesh topology

The study of Cui et al. [6] and Alghamdi et al. [7] has implemented a blockchain on a WSN as a cluster with a star topology. They suggest that dividing WSN devices into clusters will make blockchain integration easier. Their schemes have better performance results. However, blockchain implementation cannot be applied directly to the star topology. So, the message exchange mechanism needs to be modified to run on a star topology.

Figure 7 shows the ideal modification of the message exchange mechanism proposed by the researcher so that Proof-of-Authority can be optimal in a star topology. Nodes will be divided into two types: ordinary nodes that will serve as authorities and base stations as intermediaries for each node to communicate and validate. The ordinary node will be connected directly to the base station, which is assumed to have no problem with limited resources. Thus, ordinary nodes are not burdened by communication between nodes.

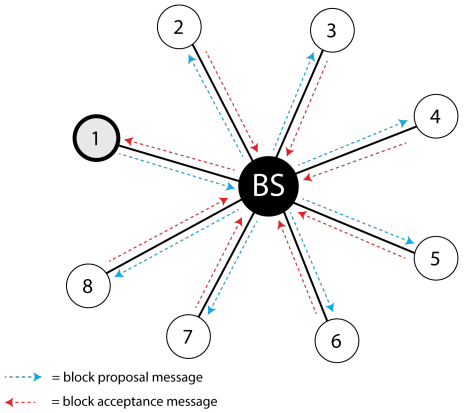


Figure 7: Ideal message exchange for WSN

4 Result and Discussion

4.1 Message Exchange Compatibility

Aura has a proposal block message exchange process - block acceptance - accept, as shown in Figure 8 When the message exchange process starts, Leader of the ordinary node will distribute the proposal block message to all nodes through the base station.

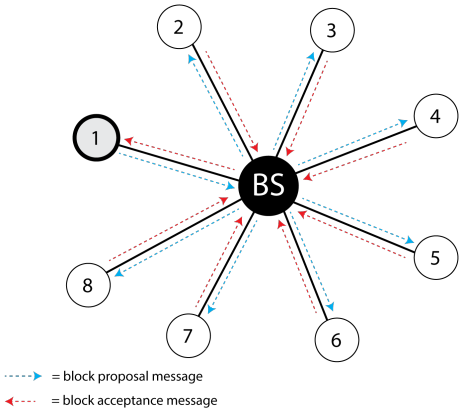


Figure 8: Aura algorithm message exchange scheme on WSN

Subsequently, the base station will distribute the message to all nodes and give a reply (block acceptance) to the Leader node, and the block status will change to “accept”. Each node will validate and enter the block into the blockchain. Assuming the base station has no limit on computing and energy resources than WSN nodes, this scheme can apply to clustered WSN. However, a message exchange scheme like this will cause scalability problems. Scalability occurs because the more node members, the more time it will take to distribute and validate from the node to the base station.

Figure 9 shows a schematic of the clique algorithm for exchanging messages in a star topology. The advantage of implementing Clique in this topology is that it has a number of $N(N/2+1)$ Leaders who can propose blocks simultaneously. In addition, the message exchange process on Clique is also shorter than Aura based on Figure 1, where Clique does not require the block acceptance stage. Thus, at one time there are several Leaders who enter blocks into the network and a short message exchange process and increase the transaction throughput. However, Clique has a very fatal drawback for WSN which makes the block unable to enter the network due to the formation of a fork. According to the GHOST protocol, only blocks from the main Leader can enter the network, and blocks from other Leaders will be discarded.

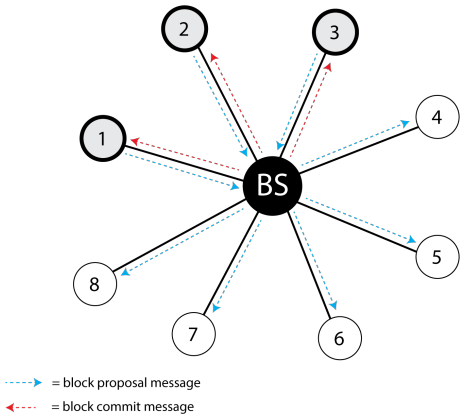


Figure 9: Clique algorithm message exchange scheme on WSN

Unfortunately, the execution of the GHOST protocol is not suitable for its application to WSN because WSN will always continue to provide valuable data. If some data from its members is discarded during the block proposal process, it will reduce the essence of implementing WSN itself. Thus, the mechanism of the Clique is not optimal compared to AuRa because it wastes valuable information. The best solution for this implementation is to modify or replace the GHOST protocol to have a function to have a block queue, so that proposed blocks from sub-Leaders are not discarded.

4.2 Performance Evaluation

4.2.1 Transaction time. Transaction time on a blockchain network is the time it takes for a blockchain system to validate transactions. In the permissioned blockchain, we can set the block interval as needed so that the block speed will be static, but the message exchange mechanism affects the transaction speed in the Aura and Clique algorithms. We can see the comparison of transaction speed in Figure 10.

Aura's transaction time is longer than Clique's on each node, as shown in Figure 10, in 100 transactions, Aura has an average transaction time of 31.62 ms, while Clique has an average transaction time of 6.03 ms. This is because the Aura scheme requires block acceptance, as shown in Figure 1, during block verification, while Clique does not. So, the more nodes, the higher the time to exchange messages on Aura. Meanwhile, Clique has a faster transaction time because it only requires a proposal block during the message exchange process.

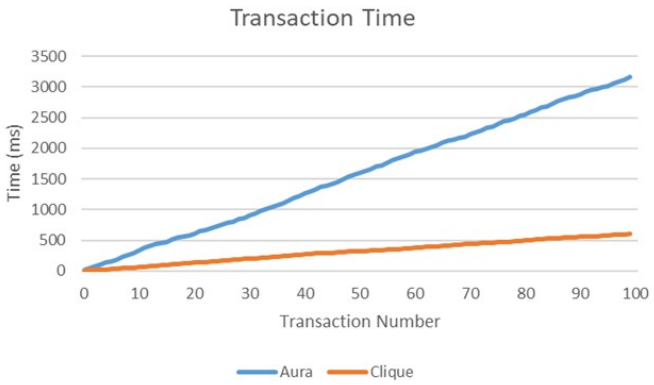


Figure 10: Transaction speed comparison

4.2.2 Transaction Drop. Transaction Drop is transaction data in the queue that is deleted and does not enter the blockchain network. On the WSN network, data will be represented by transactions continuously entered into the blockchain, which can trigger a transaction drop on the blockchain network. The comparison of transaction drops can be seen in Figure 11. Aura had no dropped transactions. All transactions submitted by each authority have been successfully verified (mined).

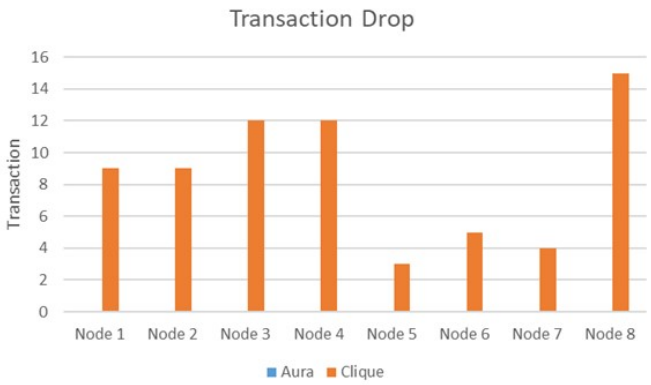


Figure 11: Transaction drop comparison

This is because Aura only rotates one Leader who can propose for a block at every step, so there are very few forks. Meanwhile, Clique had 69 transactions drop out of 800 transactions that had been entered or about 8 percent of transaction drops, as shown in Figure 6. Clique allows blockchain networks to have $N(N/2+1)$ Leader. At each step, several authorities can submit blocks simultaneously.

In Clique, if a fork occurs, the GHOST protocol will be executed, which only includes the proposed block from the

Leader, while the proposed block from the sub-leader will be discarded. Each block on Clique contains three transactions. So, the number of transaction drops that occur is the number of blocks multiplied by three.

Based on the evaluation results, both consensuses have advantages and disadvantages to WSN. However, Aura will be easier to develop for its integration to clustered WSN than Clique. Aura's message exchange mechanism can be implemented on WSN. Other than that, Aura had no problems with Fork formations. However, modifying the message exchange mechanism is necessary to improve the transaction time.

On the other hand, Clique has more challenges in its application to clustered WSN. Although the transaction speed is high, if the incoming data is not intact by all nodes, it will be a problem with WSN technology. This happens because the GHOST protocol on Clique will remove blocks that contain valuable data, which is the main essence of WSN technology.

5 Conclusion and Future Works

This research has carried out the integration of blockchain technology using Proof-of-Authority on WSN. Block generation is proven to be faster and uses less power when PoA is used. In addition, monitoring and management of network members can be carried out using PoA consensus. The comparison results show that Aura has a Transaction time of 31.62 ms / 100 transactions, while Clique has 6.03 ms / 100 transactions. Even though Aura's transaction speed is slower, Aura doesn't have any wasted blocks, as with Clique, which has about 8 percent of the total transactions. The term "transaction" in the WSN system is input data such as sensor data, monitoring data, and image data categorized as valuable and resulting from environmental observations from WSN devices. Losing a transaction on the blockchain system integrated with the WSN is a shortcoming that removes the essence of the WSN technology itself. Thus, Aura is more suitable to apply to WSN compared to Clique.

For future work, researchers will continue to implement and adapt the peer-to-peer blockchain into a star topology (WSN cluster) to produce a Proof-of-Authority design that can be optimally applied to WSN.

Acknowledgments

This work is supported by the Indonesian Government Scholarship PMDSU Grant number NKB-3046/UN2.RST/HKP.05.00/2020 from the Ministry of Research, Technology, and Higher Education (Kemristekdikti).

References

[1] N. S. Alghamdi and M. A. Khan, "Energy-Efficient and Blockchain-Enabled Model for Internet of Things (IoT) in Smart Cities," *CMC-Computers Materials Continua*, 66(3):2509-2524, 2021.

[2] "Aura." [Online]. Available: https://openethereum.github.io/Aura, 2022.

[3] G. Ayoade, K. Hamlen, V. Karande, and L. Khan, "Decentralized IoT Data Management Using Blockchain and Trusted Execution Environment," in 2018 IEEE International Conference on Information Reuse and Integration (IRI), IEEE, pp. 15-22, 2018.

[4] M. Banerjee, J. Lee, and K.-K. R. Choo, "A Blockchain Future for Internet of Things Security: A Position Paper," *Digital Communications and Networks*, 4(3):149-160, 2018.

[5] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A Scalable Blockchain Framework for Secure Transactions in IoT," *IEEE Internet of Things Journal*, 6(3):4650-4659, 2018.

[6] S. M. Bozorgi and A. M. Bidgoli, "HEEC: A Hybrid Unequal Energy Efficient Clustering for Wireless Sensor Networks," *Wireless Networks*, 25(8):4751-4772, 2019.

[7] V. Buterin, "Ethereum: Platform Review," Opportunities and Challenges for Private and Consortium Blockchains, 2016.

[8] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery," *ACM Transactions on Computer Systems (TOCS)*, 20(4):398-461, 2002.

[9] "Clique." [Online]. Available: https://github.com/ethereum/EIPs/issues/225, 2022.

[10] Z. Cui, X. Fei, S. Zhang, X. Cai, Y. Cao, W. Zhang and J. Chen, "A Hybrid Blockchain-based Identity Authentication Scheme for Multi-WSN," *IEEE Transactions on Services Computing*, 13(2):241-251, 2020.

[11] B. Curran, "What is Proof of Elapsed Time Consensus?(PoET) Complete Beginner's Guide," ed: Blockonomi. url: https://blockonomi. com/proof-ofelapsed-time-consensus, 2018.

[12] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain," Italian Conference on Cyber Security, 2018.

[13] V. Dedeoglu, R. Jurdak, G. D. Putra, A. Dorri, and S. S. Kanhere, "A Trust Architecture for Blockchain in IoT," in Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, pp. 190-199, 2019.

[14] G. Dittmann and J. Jelitto, "A Blockchain Proxy for Lightweight IoT Devices," in 2019 Crypto Valley Conference on Blockchain Technology (CVCBT), IEEE, pp. 82-85, 2019.

[15] F. M. Enescu, N. Bizon, A. Cirstea, and C. Stirbu, ”Blockchain Technology Applied in Health the Study of Blockchain Application in the Health System (I),” in 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), IEEE, pp. 1-4, 2018.

[16] T. Frikha, A. Chaari, F. Chaabane, O. Cheikhrouhou, and A. Zaguia, ”Healthcare and Fitness Data Management Using the IoT-based Blockchain Platform,” *Journal of Healthcare Engineering*, 2021:12 pp, 2021.

[17] ”Go Ethereum.” [Online]. Available: https://github.com/ethereum/go-ethereum, 2021.

[18] F. . Hjálmarsson, G. K. Hreiarsson, M. Hamdaqa, and G. Hjálmtýsson, ”Blockchain-Based E-Voting System,” in 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), pp. 983-986, 2-7 July 2018.

[19] M. A. Islam and S. Madria, ”A Permissioned Blockchain Based Access Control System for IoT,” in 2019 IEEE International Conference on Blockchain (Blockchain), pp. 469-476, July 2019.

[20] T. Kim, J. Noh, and S. Cho, ”SCC: Storage Compression Consensus for Blockchain in Lightweight IoT Network,” in 2019 IEEE International Conference on Consumer Electronics (ICCE), IEEE, pp. 1-4, 2019.

[21] S. Nakamoto, ”Bitcoin: A Peer-to-Peer Electronic Cash System.” Decentralized Business Review: 21260, (2008).

[22] D. Ongaro and J. Ousterhout, ”In Search of an Understandable Consensus Algorithm,” in 2014 USENIX Annual Technical Conference (Usenix ATC 14), pp. 305-319, 2014.

[23] ”OpenEthereum.” [Online]. Available: https://github.com/openethereum/openethereum, 2021.

[24] V. B. Pavel Khahulin Igor Barinov, ”PoA Network White Paper,”. [Online]. Available: https://github.com/poanetwork/wiki/wiki/POA-Network-Whitepaper, 2018.

[25] P. K. Singh, R. Singh, S. K. Nandi, and S. Nandi, ”Managing Smart Home Appliances with Proof of Authority and Blockchain,” *International Conference on Innovations for Community Services*, Springer, pp. 221-232, 2019.

[26] P. Treleaven, R. G. Brown, and D. Yang, ”Blockchain Technology in Finance,” *Computer*, 50(9):14-17, 2017.

[27] L. Wu, W. Lu, F. Xue, X. Li, R. Zhao, and M. Tang, ”Linking Permissioned Blockchain to Internet of Things (IoT)-BIM Platform for Off-Site Production Management in Modular Construction,” Computers in Industry, 135:103573, 2022.

[28] J. Yang, S. He, Y. Xu, L. Chen, and J. Ren, ”A Trusted Routing Scheme Using Blockchain and Reinforcement Learning for Wireless Sensor Networks,” Sensors, 19(4):970, 2019.

[29] R. Zhang, J. Pan, D. Xie, and F. Wang, ”NDCMC: A Hybrid Data Collection Approach for Large-Scale WSNs Using Mobile Element and Hierarchical Clustering,”*IEEE Internet of Things Journal*, 3(4):533-543, 2015.

Delphi Hanggoro is an PhD student at Universitas Indonesia. He graduated from Computer Engineering at Diponegoro University in 2017, then continued Post Graduate at the University of Indonesia in 2018 and graduated in 2020. He is currently in the process of completing his PhD on the topic of performance improvement on consensus in the permissioned blockchain.

Jauzak Hussaini Windiatmaja has completed a bachelor’s program in Computer Science at Diponegoro University in 2018, he continued Post Graduate at the University of Indonesia in 2019 and graduated in 2021. He is currently running a PhD program at the Department of Electrical Engineering, University of Indonesia with topic integrating machine learning with blockchain.

Riri Fitri Sari She earned a Bachelor of Electrical Engineering from UI in 1994 and a Masters in Human Resources from Atmajaya University Jakarta in 1996. In 1997, she received an MSc in Software Systems and Parallel Processing from the Department of Computer Science, University of Sheffield, England with the Chevening Award from the British Council. She successfully finished her doctoral dissertation with research in the field of Active Network Congestion-Based Congestion Management and obtained her PhD from the School of Computing, University of Leeds, England. She was confirmed as a Professor in Computer Engineering in May 1, 2009, in the Department of Electrical Engineering, Faculty of Engineering, University of Indonesia. Currently, she is actively

teaching and researching in the fields of Computer Networking, Grid Computing, Information and Communication Technology implementation. From various scientific publications in the form of international journals and presentations at various electrical and computer engineering conferences in various countries and achievements in the application of information technology, Riri Fitri Sari was chosen to be a Senior Member of the Institute of Electronics and Electrical Engineers (IEEE).

An Efficient Maximal Free Submesh Detection Scheme for Space-Multiplexing in 2D Mesh-Connected Manycore Computers

Ismail Ababneh* and Saad Bani-Mohammad*
Al al-Bayt University, Mafraq 25113, JORDAN

Abstract

For multicore systems, space-sharing (space-multiplexing) is a promising core allocation strategy as the number of cores grows into the hundreds and thousands because it can achieve scalability and good system performance. In space-multiplexing, an application is allocated its own set of cores for the duration of its execution. In this paper, we propose a new efficient maximal free submesh detection scheme for two-dimensional mesh-connected manycore systems. Free submeshes that are not contained in other free submeshes are detected and placed in a free-list for direct support of space-multiplexing. An advantage of the proposed scheme is that its time complexity is quadratic in the number of free submeshes, whereas the time complexity of the previous such scheme is cubic in this number. In addition to complexity analysis, detailed simulations are carried out to evaluate the proposed scheme. In the simulations, we consider several approaches to selecting allocation submeshes from the free-list. The approaches range from a promising first-fit variant to a scheme that aims to keep large free submeshes for future allocation requests. The results show that the proposed scheme is substantially more time-efficient than the previous cubic recognition-complete maximal free submesh scheme. It achieved up to seventy percent reduction in the average combined allocation and de-allocation times in these simulations.

Key Words: Manycore systems, mesh interconnection network, space-sharing (space-multiplexing), maximal free submesh, contiguous submesh allocation.

1 Introduction

Over the past two decades, there has been, mainly because of the power wall, a shift from increasing the clock frequency of single-thread microprocessors to multicore processors, where several cores or processing units are built on a single chip. As per Moore's law, it has also been possible to incorporate many cores and build manycore processors, which are multicore systems with many relatively simple cores that can support high explicit parallelism.

For communication among the cores in manycore systems, a Network-on-Chip (NoC) architecture is used. This is to avoid the bottleneck problem that the bus interconnection architecture suffers from when the number of cores becomes large. The mesh is a popular NoC interconnection topology, in both its two-dimensional (2D) and three-dimensional (3D) forms [16, 17, 24]. An example is the 2D 8×10 mesh network of an 80-core Intel manycore research chip, where each core or Processing Element (PE) is associated with a 5-port router for communication [23]. Four ports are used for communicating with the four neighbors of internal cores. Cores on mesh corners and on its edges have fewer neighbors. The fifth port is for NoC-PE communication. Another example is the TRIPS OCN that has a 4x10 wormhole-routed 2D mesh interconnection network [11]. A recent 1024-node manycore system has the mesh topology, and comprises 32 clusters, where a cluster is a 4×8 mesh. To decrease the system's diameter, each cluster has in its middle a Radio Hub (RH) that communicates with the four 2D routers of the middle cluster node. Communication among clusters takes place via the RHs. Within clusters, communication uses the mesh interconnection network [13]. In [17], a NOC that combines ring and 2D mesh interconnections and adapts to application requirements is proposed for improved scalability and energy efficiency up to 1024 processing elements.

Several studies indicate that space-multiplexing (space-sharing) is a promising core allocation strategy for manycore systems, as it can achieve scalability and good performance for large core numbers [22, 25]. By allocating resources spatially, traditional time multiplexing scheduling is transformed into a layout and partitioning problem, where jobs or applications, including possibly the OS, run on their own sets of cores. In space-sharing, a job can be executed on a submesh of the manycore system, which can reduce communication distances, interference among jobs, message delays, energy consumption and chip temperatures. Supporting this, previous studies have shown that mapping the communicating tasks of a parallel job to neighboring cores, in particular the cores of a single submesh, can reduce communication delays and power consumption, and improve throughput and job execution times [5, 8, 18].

Based on this, we assume that allocation is contiguous, where a job requests and is allocated a single submesh of a width and a height that the job specifies. By running on a single submesh, the job can achieve reduced distances among the cores it is allocated. Also, a space-sharing allocation policy is required to achieve high system utilization. It must be capable of detecting all free core submeshes and should aim to maximize the number of allocated cores (i.e., minimize core fragmentation) [9, 15, 26]. In addition, it must be time-efficient, especially as the system size (i.e., number of cores) of the manycore system grows. Migratory space-sharing policies that carry out defragmentation of scattered submeshes that result when jobs exit the system have been considered. An issue in these policies is when to carry out

* Computer Science Department, Prince Hussein Bin Abdullah Faculty of Information Technology. Emails: ismael@aabu.edu.jo and bani@aabu.edu.jo.

defragmentation and the associated job migrations, the cost of migration, and application size constraints imposed by some of these policies to simplify defragmentation [19, 20]. Such constraints can result in internal fragmentation.

Several contiguous space-sharing allocation policies were proposed for multicomputers with 2D mesh interconnection topologies. Several of these policies do not scale well. They have time complexities that grow with the system size (its number of PEs) [7, 10, 26, 27]. However, more efficient policies that build lists of free submeshes and/or allocated submeshes were proposed. The allocation decisions they make are based on the elements in these lists, and their time complexities are functions of list sizes [1, 6, 9, 12, 14]. A major advantage of such policies is that list sizes can be much smaller than system sizes [1, 3].

An advantage of submesh allocation that is based on *free* submeshes is its flexible submesh selection. When multiple large-enough free submeshes exist, they all can readily and simply be considered for allocation to the current request, which can lead to superior allocation. A free-list allocation policy that can detect all *maximal* free submeshes in a 2D mesh system has been proposed [12]. However, the submesh detection algorithm it uses is not efficient. It has time complexity that is cubic in the number of free submeshes. A free submesh is *maximal* if it is not contained in another free submesh. More efficient algorithms for building the free-list have been proposed [1, 14]. However, they are not recognition-complete. They fail to detect some available submeshes, which can result in unsuccessful allocation to the current allocation request although there is in fact at least one large-enough free submesh for satisfying this request.

In this paper, we propose an efficient recognition-complete maximal free submesh detection scheme for 2D mesh-connected manycore systems. An advantage of this scheme over the previous recognition-complete scheme, proposed in [12], is that its time complexity is quadratic in the number of free submeshes, while the time complexity of the previous scheme is cubic in this number. Using detailed simulations, we evaluated and compared these two detection schemes. In these simulations, various previous promising policies for deciding where allocation will take place are considered. They range from a promising first-fit variant [10] to a policy that aims to keep large free submeshes for future allocation using a reservation function [12], and a policy that gives priority to mesh corner then peripheral allocation [3]. Corner and peripheral placements have for goal leaving large free submeshes for future allocation. The simulation results show that when allocation and de-allocation times are considered, the proposed submesh detection scheme substantially outperforms the previous maximal free submesh detection scheme. It has achieved up to seventy percent improvement in the measured combination of these times.

We limit our attention here to 2D meshes; however, this work can be adapted for 3D meshes. This paper is organized as six sections. Section 2 below contains a few preliminaries. Section 3 has a review of related schemes. The proposed detection scheme is defined and analyzed in Section 4. The system model, and simulation parameters and results are in Section 5. Finally, Section 6 contains the research conclusions.

2 Preliminaries

The target manycore system, M(W, H), is of width W and height H. A core is denoted by the coordinates (i, j), where $1 \leq i \leq W$ and $1 \leq j \leq H$. Cores are interconnected by bidirectional communication links as shown in Figure 1. The size of the mesh is the number of its cores, N, where N=W*H.

A w × h submesh is represented by a 4-tuple (i1, j1, i2, j2), where (i1, j1) represent its base node, and (i2, j2) its end node. We have that w = i2 – i1 + 1 and h = j2 – j1 + 1. In Figure 1, (1, 3, 3, 4) represents the 3 × 2 submesh S_1.

A submesh is said to be free if none of its cores is allocated. As indicated previously, a free submesh is said to be *maximal* if it is not contained in another free submesh. Also, a submesh is said to be busy or allocated if all its cores are allocated to the same job. In Figure 1, the maximal free submeshes are (1, 1, 1, 4), (1, 3, 5, 4), and (3, 1, 5, 4). For example, (3, 1, 5, 2) is not maximal as it is contained in (3, 1, 5, 4). If the cores (2, 1) and (2, 2) in Figure 1 are allocated to the same job, then (2, 1, 2, 2) is a busy or allocated submesh.

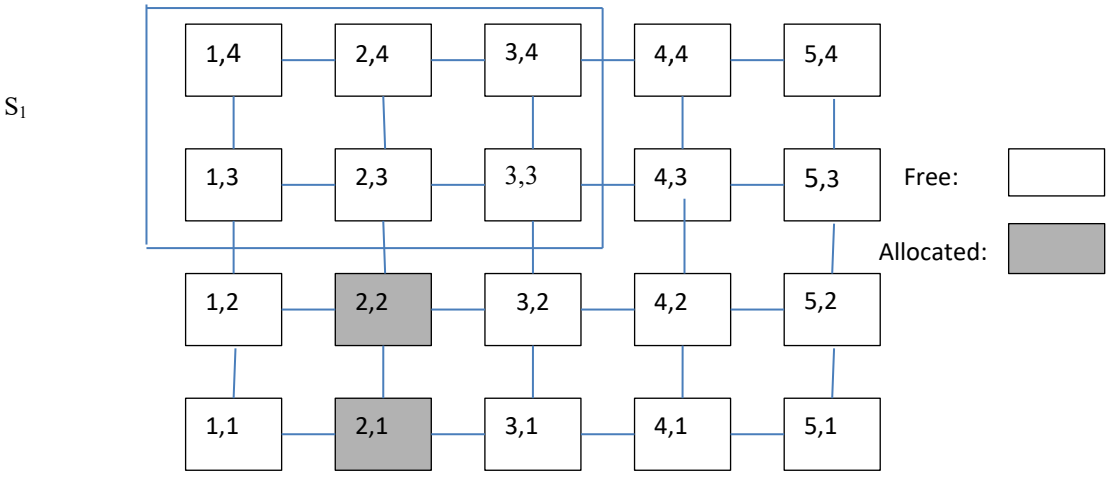


Figure 1. M(5, 4) 2D mesh

3 Previous Works

Several contiguous allocation policies based on free and/or busy submeshes have been proposed for 2D meshes. They differ in how they detect free submeshes, how they select a free submesh for allocation, and where the allocated submesh is located within the free submesh selected. A major aim of a contiguous allocation policy should include reducing external fragmentation. That is, reducing the number of free cores that remain idle although they are sufficient in number to satisfy the allocation request of the job that the scheduling algorithm has selected for execution. For instance, a policy may fail to detect some of the free submeshes, and it may make some poor placement choices that result in a relatively large number of small free submeshes, rather than fewer large ones. In what follows, N is the size of the target manycore system, and f and b are the numbers of free and busy submeshes, respectively. We also assume that a job's allocation request upon arrival is for an $\alpha \times \beta$ free submesh, where the width and height of the submesh requested are α and β.

3.1 Busy-List with Global Adjacency (BLGA)

This policy [9] uses a list of allocated processors. It attempts to satisfy the allocation request in its $\alpha \times \beta$ or $\beta \times \alpha$ orientations using a submesh that has the largest number of adjacent busy cores and mesh boundary cores. The rationale is that this can reduce fragmentation. The time complexity of allocation in BLGA is in $O(b^3)$, and that of de-allocation is in $O(1)$. In [28], a BLGA improvement that aims to allocate adjacent submeshes to requests served close in time is proposed. However, such heuristic assumes that jobs that start execution close in time tend to have close exit times.

3.2 Free-List with First-Fit Adjacency (FLFFA)

This scheme [14] builds a free-list that approximates the maximal free list (MFL), and a busy-list. The free-list elements are sorted in the non-decreasing order of their shorter edge. The first free submesh that can accommodate the current allocation request as $(\alpha \times \beta)$ or $(\beta \times \alpha)$ is the allocation candidate. Allocation for both orientations is considered in the corners of the candidate submesh, and a placement with the maximum number of adjacent busy cores and mesh peripheral cores is the allocation submesh. The number of adjacent busy processors is computed using the busy-list. FLFFA was compared to BLGA using simulations, where it achieved superior waiting delays. Also, FLFFA outperformed BLGA overall in another simulation study [12].

The allocation and de-allocation operations have $O(f^2)$ time complexities. In [1], an $O(f)$ heuristic for approximating MFL has been proposed. In both heuristics, building the free-list starts with expanding, if possible, the released submesh into the current elements of the free-list when a job terminates. This step produces new free submeshes. Then, expansions of the current elements into the new submeshses are attempted. The expanded and new submeshes are used in forming the new free-list. A problem is that this approach is not recognition-complete, as can be seen in Example 1 below.

Example 1. In Figure 2, if the job running on (2, 1, 2, 4) terminates, the released submesh cannot be expanded into the existing free submeshes ({(1, 1, 1, 2), (3, 1, 5, 2)}), and the new free submesh is {(2, 1, 2, 4))}. Then, (1, 1, 1, 2) is expanded into (2, 1, 2, 4) to produce the free submesh (1, 1, 2, 2). Likewise, expanding (3, 1, 5, 2) into (2, 1, 2, 4) produces (2, 1, 5, 2). Thus, (1, 1, 5, 2) is not detected, and the detected submeshes (1, 1, 2, 2) and (2, 1, 5, 2) are not maximal as they are proper submeshes of the undetected maximal free submesh (1, 1, 5, 2).

3.3 Reservation Best-Fit (RBF)

This policy [12] builds the MFL and sorts its elements in their non-increasing size order. The submesh size is the number of cores it contains. The policy also builds a busy list. The MFL is scanned for large enough free submeshes. In these submeshes, all possible $\alpha \times \beta$ and $\beta \times \alpha$ submesh corner placements are considered candidate submeshes. A reservation function is employed for computing leftover free submeshes with the aim of preserving large free submeshes for later use. Using simulations, RBF outperformed FLFFA

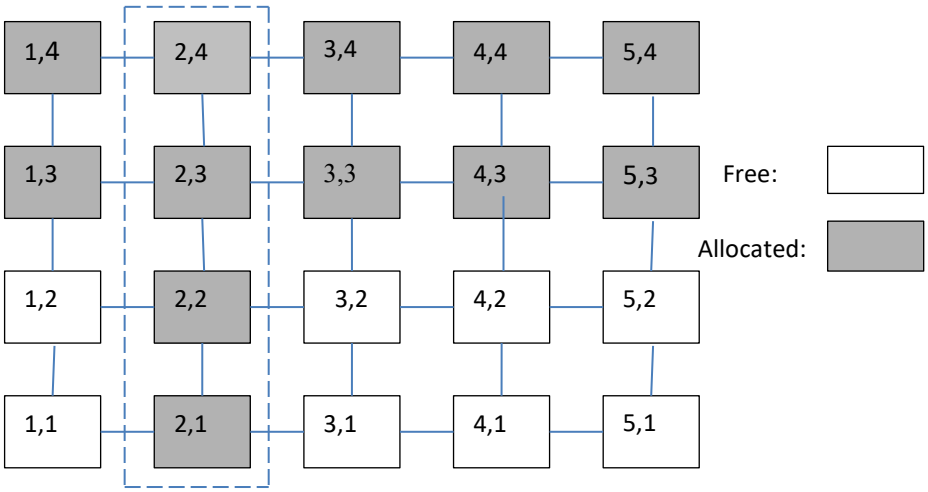


Figure 2. An example illustrating incomplete recognition

and BLGA in terms of average job waiting delays [12]. The time complexity for building MFL upon a job exit is in $O(f^3)$, and that needed upon an allocation operation is in $O(f^2)$. Both use submesh subtraction operations, instead of expansions.

3.4 Right Border Line (RBL)

This strategy [6] keeps a busy-list and uses it to determine the allocation right border lines. These lines consist of nodes that can serve as bases for the current allocation request. By construction, the lines either have to their left an allocated submesh or they are the left boundary of the mesh itself. A policy that re-builds the RBLs and looks for an allocation RBL for $\beta \times \alpha$ when none is found for $\alpha \times \beta$ was also proposed. In both cases, the upper end core of the first allocation RBL to be found is chosen as base node for the allocated submesh. The allocation time of RBL is in $O(b^2)$, and that of de-allocation is in O(1). Using simulations, the performance of the orientation-switching RBL policy was evaluated and compared to the performance of BLGA and several other allocation policies. The policies considered produced almost similar average job waiting delays, with BLGA performing slightly better than the others [6].

4 Proposed Submesh Detection Scheme

In the free submesh detection scheme proposed in this paper, the maximal free submeshes are found and form an unordered *MFL*. Initially, this list contains the entire mesh. It is then reconstructed after each job departure (i.e., submesh release), and each allocation.

4.1 Detection of Maximal Free Submeshes upon De-allocation

When a job terminates and the submesh it is allocated is released, an attempt is made first to expand the released submesh into the current elements in *MFL* using two patterns. The first is a horizontal-vertical expansion, and the second is a vertical-horizontal expansion. In horizontal expansion, a submesh may expand into a free submesh located to its left or right. In vertical expansion, the expanded into submesh may be above or below the expanding submesh. At most two new different submeshes can result from these expansions. The first is generated by the horizontal-vertical expansion, and the second is generated by the vertical-horizontal expansion. If expansion is not possible, the only new submesh is the released submesh itself. In all cases, if an expanding submesh covers an expanded into submesh after the expansion, the latter is removed from *MFL* because its free cores are covered. The expansions of the released submesh into the elements of *MFL* are of the complete type, as defined below [1].

Definition 1. A free submesh (i1, j1, i2, j2) is *completely* expandable right into an adjacent free submesh (i3, j3, i4, j4) if $i2 \geq i3 - 1$, $i2 < i4$, $i1 < i3$, $j2 \leq j4$, and $j1 \geq j3$. This expansion turns (i1, j1, i2, j2) into (i1, j1, i4, j2). Complete expansions down, up, and left are defined similarly. If j2 = j4 and j1 = j3, we have that (i3, j3, i4, j4) $\subset$ (i1, j1, i4, j2). When (i3, j3, i4, j4) is an element of *MFL*, it is removed because its free cores are in (i1, j1, i4, j2). Expansions in the remaining directions are handled similarly.

Example 2. In Figure 3, *MFL* = {(4, 3, 5, 4), (1, 3, 5, 3), (3, 1, 3, 3)}. Assume S = (1, 4, 3, 4) is released. The horizontal step of the horizontal-vertical complete expansion of S into the elements of MFL produces (1, 4, 5, 4) by the complete expansion of S into (4, 3, 5, 4), then (1, 4, 5, 4) becomes (1, 3, 5, 4) by its complete expansion into (1, 3, 5, 3) in the vertical step and (1, 3, 5, 3) is removed.

As a result of the release of a submesh and its expansions, it may be possible to expand *MFL* elements completely or partially (see Definition 2 below) into the new submeshes to produce larger or additional free submeshes. This expansion is conducted next. If an edge of a submesh in *MFL* is partially or completely covered by or borders a new submesh, the submesh or parts of it are extended to the other end of the new submesh. An element in *MFL* that is covered by one of the new submeshes before or after expansion is removed from this list.

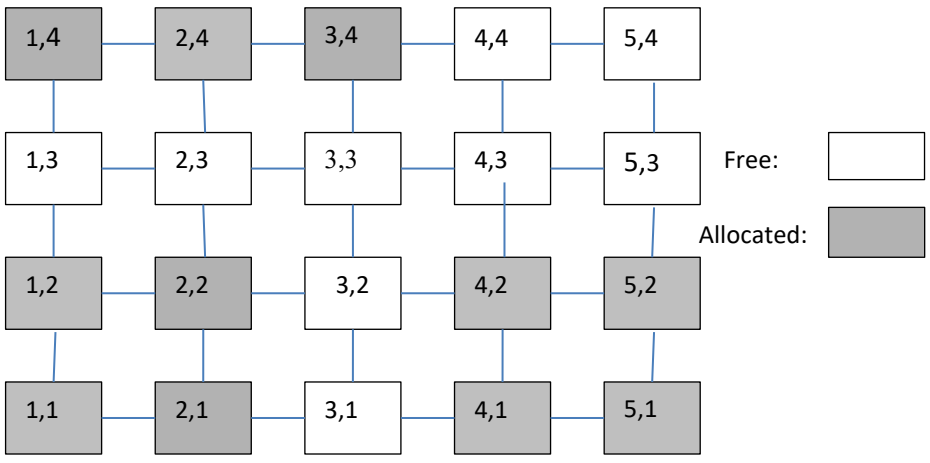


Figure 3: Submesh release example

Example 3. Continuing with Example 2. The new free submesh is (1, 3, 5, 4), and the submeshes that remain in *MFL* are (3, 1, 3, 3) and (4, 3, 5, 4). The submesh (4, 3, 5, 4) is covered by (1, 3, 5, 4), therefore it is removed. The submesh (3, 1, 3, 3) is expanded completely into (1, 3, 5, 4), producing the maximal free submesh (3, 1, 3, 4).

Definition 2. The partial expansion of a free submesh into a second one is the horizontal and/or vertical expansion of the largest subpart(s) of this free submesh into the second one.

Example 4. If the submesh (5, 4, 6, 5) in Figure 4 is released, the part (5, 1, 5, 3) of (4, 1, 5, 3) is expanded partially into (5, 4, 6, 5), producing (5, 1, 5, 5). Also, (5, 6, 5, 6) is completely expanded into (5, 4, 6, 5) to produce (5, 4, 5, 6).

It can be noticed that the free submesh (5, 1, 5, 6) in Example 4 is not detected by the expansions considered so far. Partial and complete expansions across the released submesh are needed. To carry out such expansions, the free submeshes must be processed further for possible inter-expansions. For example, (5, 1, 5, 5) can be expanded completely into (5, 4, 5, 6) to produce the maximal free submesh (5, 1, 5, 6). In this expansion, the expanded into submesh is removed because it is covered by the result of the expansion. In all cases, a free submesh is removed and does not appear in the final *MFL* if it is covered by any other free submesh.

Another reason for missing maximal free submeshes by the expansions considered so far is the existence of free submeshes around a corner of the released submesh or its expansions. A maximal free submesh is missed if the sides of corner free submeshes are shorter than the sides they face in the released submesh or its expansion. For example, if the submesh (2, 2, 3, 4) is released in Figure 4, then the partial expansions of (1, 1, 1, 3) and (1, 1, 2, 1) into this submesh will produce (1, 2, 3, 3) and (2, 1, 2, 4). However, (1, 1, 2, 3) is not detected. To detect this maximal free submesh, (1, 1, 2, 1) should be expanded into (1, 2, 3, 3). Finally, once these additional expansions are carried out the detected free submeshes should be processed for coverage. In the current example, (1, 1, 2, 3) covers (1, 1, 1, 3), therefore the latter submesh is removed. The complete de-allocation algorithm is in Figure 5.

For analyzing this de-allocation algorithm, it can be seen that the number of possible complete expansions in Step 2 is in O(f). Also, because of the generation of $S1$ and $S2$ the number of free submeshes at the end of Step 2 is at most $f + 2$. As a result of the partial and complete expansions in Steps 3 and 4, the number of known free submeshes at the end of these steps is also in O(f). The number of tests needed for coverage detection and processing in Step 6 is in O(f^2). After this coverage detection, the number of free submeshes detected is in O(f) because only a subset of maximal free submeshes has been detected so far. Consequently, the number of operations needed in Step 7 is in O(f^2).

Upon completion of Step 7, the maximal free submeshes that are generated by the partial and complete expansions across the released submesh are detected. Also, are detected the additional maximal free submeshes associated with the corner free submeshes. Intuitively, the number of additional maximal free submeshes detected in Step 7 is in O(f), and the number of tests needed for coverage detection and processing in Step 8 is in O(f^2). It is easy to see that Steps 1 and 5 take constant time. Hence, the complexity of this algorithm is in O(f^2).

4.2 Detection of Maximal Free Submeshes upon Allocation

Upon allocation, a selection scheme that determines the submesh where allocation will take place, such as first-fit, is employed. Then, where allocation takes place in this submesh is determined. This placement could, for example,

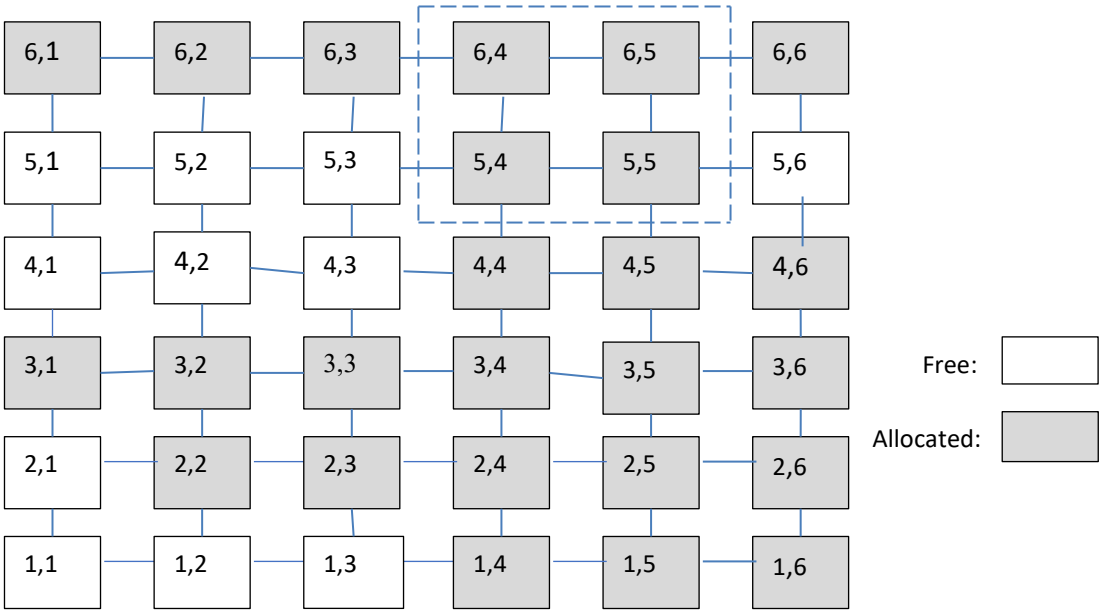


Figure 4: Submesh release example

Procedure de-allocate(S) /* An allocated submesh S is released */
Step 1) *num_free_cores* += size(S) /* update the number of free cores */
S_1=S; S_2=S
Step 2) Completely expand S_1 horizontally into the elements of *MFL*
Completely expand S_2 vertically into the elements of *MFL*
Completely expand S_1 vertically into the elements of *MFL*
Completely expand S_2 horizontally into the elements of *MFL*
$R = S_1$
Step 3) for each submesh F in *MFL* {
if F is outside R and they are not adjacent go to next F
else if $F \subseteq R$ remove F from *MFL*
else if no node in F is adjacent to a node in S go to next iteration of this loop else if complete expansion of F into R is possible {
completely expand F into R (down, right, up, or left)
if $R \subseteq F$ then $R = F$ and remove F from *MFL*
}
else if partial expansion from F into R is possible
form resulting fragments and add them at the head of a temporary list *TL*
else completely expand R into F (up, right, left, or down) if possible
}
Step 4) repeat Step 3) for $R = S_2$ if $S_2 \neq S_1$
Step 5) Append *TL* at the head of *MFL* to form the list *FL*: *FL* = *TL* + *MFL*
TL = ∅
Step 6) /* Remove *FL* elements that are non-maximal: */
for each element S_i in *FL*
for each element S_j that is after S_i in *FL*
if ($S_j \subseteq S_i$) remove S_j from *FL*
else if ($S_i \subseteq S_j$) mark S_i for removal before going on to the next S_i
Step 7) /* Carry out expansions across the released submesh and around corners */
Carry out all additional complete and partial expansions among *FL* elements
Add the fragments that result from partial expansions at the head of *TL*
Step 8) *FL* = *TL*+*FL*; Remove non-maximal *FL* elements; *MFL* = *FL*; *TL* = ∅
} /* end of procedure de-allocate */

Figure 5: The de-allocation algorithm

be in the lower-left or lower-right corner of the allocation submesh. Then, *MFL* is rebuilt. The allocation submesh is removed from *MFL* and the fragments that result from the subtraction of the allocated submesh from it are added at the head of a temporary list, *TL*. Also, the allocated submesh is subtracted from overlapping *MFL* elements, and the results are added at the beginning of *TL*. Finally, *TL* is appended at the head of *MFL*. The list that results is scanned, and a submesh in this list is removed if it is covered by another element in the list. Thus, the elements that remain in the list are maximal, and they constitute the new *MFL*. The allocation algorithm is given in Figure 6.

/* Current job requests the allocation of an $\alpha \times \beta$ submesh */
Procedure allocate (α, β){
Step 1) if *num_free_cor* < $\alpha\beta$ return Failure
Step 2) Select an allocation submesh S from *MFL*, and position the allocated submesh A within S
if no S is found return Failure
Step 3) Remove S from *MFL*
Step 4) Subtract A from S
Step 5) Add fragments that result from the subtraction at the head of a temporary list *TL*
Step 6) for each submesh S_i in *MFL*
if S_i overlaps with A{
Remove S_i from *MFL*
Subtract the overlapping part $A \cap S_i$ from S_i
Add the resulting fragments at the head of *TL*
}
Step 7) Append *TL* at the head of *MFL* producing a list *FL*
Step 8) Remove *FL* elements that are non-maximal
Step 9) *num_free_cores* = *num_free_cores* - $\alpha\beta$; *MFL* = *FL*; return Success
} /* end of procedure allocate */

Figure 6: Allocation algorithm

The subtraction operation used in the allocation algorithm is one that produces maximal difference submeshes. For example, subtracting (1, 1, 2, 2) from (1, 1, 5, 4) in Figure 7 yields the fragments (3, 1, 5, 4) and (1, 3, 5, 4). The subtraction of (3, 2, 4, 3) from (1, 1, 5, 4) produces the four difference submeshes (1, 1, 5, 1), (1, 1, 2, 4), (1, 4, 5, 4), and (5, 1, 5, 4), as another example.

Example 5. This example illustrates how allocation works. Assume a free system, and a request for a 2 × 2 submesh arrives. Initially, *MFL* consists of the whole mesh (1, 1, 5, 4). If the request is allocated (1, 1, 2, 2), then (1, 1, 5, 4) is removed from *MFL*, and the subtraction of (1, 1, 2, 2) from (1, 1, 5, 4) yields the fragments (3, 1, 5, 4) and (1, 3, 5, 4), which are added at the head of *TL*. Then, *TL* is appended at the head of *MFL* to produce *FL* = {(3, 1, 5, 4), (1, 3, 5, 4)}. This is the final *MFL* because all its elements are maximal. If a 4 × 2 allocation request arrives, the allocation selection algorithm may choose the allocation submesh S = (1, 3, 5, 4) and allocate A = (1, 3, 4, 4). In this case, (1, 3, 5, 4) is removed from *MFL*, and the subtraction of A from S produces the fragment (5, 3, 5, 4), which is added to a new *TL*. Then A *is* subtracted from (3, 1, 5, 4), yielding the fragments (3, 1, 5, 2) and (5, 1, 5, 4), which are added to *TL*. The submesh (3, 1, 5, 4) is removed from *MFL*. Finally, (5, 3, 5, 4) is removed because it is covered by (5, 1, 5, 4). The final *MFL* is {(3, 1, 5, 2), (5, 1, 5, 4)}.

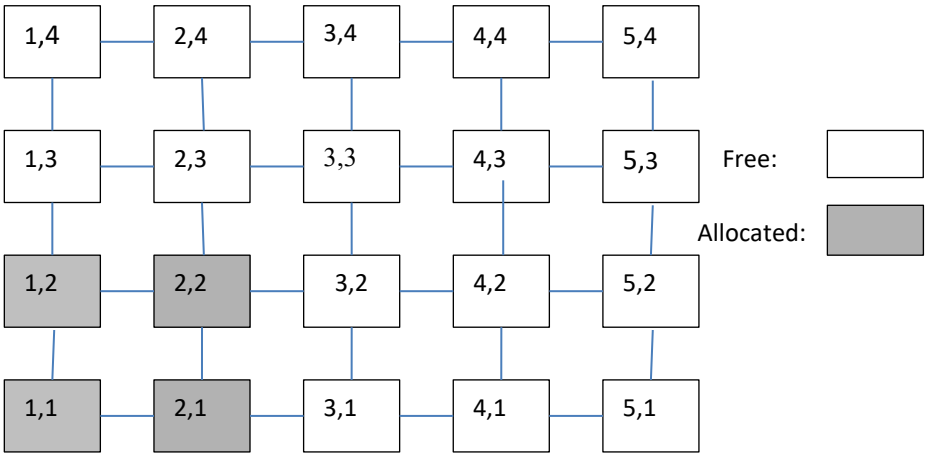


Figure 7: Subtraction and allocation example

Analyzing the allocation algorithm, we assume that a scheme that can select an allocation submesh in $O(f^2)$ time is used. The first-fit is an example of such schemes as it requires $O(f)$ steps for this selection. The number of fragments that results from subtracting the allocated submesh from the free submeshes in Step 6 is in $O(f)$; their number is at most $4f$ as the subtraction operation of a 2D submesh from another 2D submesh results in at most four submeshes. Therefore, the number of operations in Step 8 and the complexity of the algorithm are in $O(f^2)$.

4.3 Selection of Allocated Submeshes

A comparison of several policies for selecting where allocation takes place when the maximal free submesh detection scheme proposed in [12] is used can be found in an earlier work [2]. For the comparison of the maximal free submesh detection scheme that we propose to that proposed in [12], the following promising schemes for determining where allocation takes are considered:

4.3.1 Switching First-Fit (SFF). The first *MFL* element that is large enough for the current $\alpha \times \beta$ request is the allocation submesh, and the $\alpha \times \beta$ submesh in its lower-left corner is allocated for the request. If this fails, first-fit allocation is re-attempted for the $\beta \times \alpha$ orientation. Switching request sides was first proposed in [10], and it has been used in many studies [1, 3, 6, 9, 14, 26].

4.3.2 Maximum Mesh Peripheral Length (MMPL). This policy gives priority to allocating mesh corner submeshes because they have the most peripheral cores. In scanning *MFL*, if there is a corner submesh that is large enough for $\alpha \times \beta$ or $\beta \times \alpha$ request shapes, the requesting job is placed in this mesh corner in the right orientation and scanning is terminated. Any corner placement will have the most peripheral cores. If a large enough submesh in *MFL* has a side aligned with a mesh edge, the peripheral lengths associated with possible $\alpha \times \beta$ and $\beta \times \alpha$ placements are computed. When there is no corner allocation, the first placement with the most peripheral cores is assigned to the request. If no corner or peripheral placement is possible, the request is placed at the base of the first large-enough internal submesh in *MFL* [3]. A generalization of the orientation switching transformation that permits all viable request shapes has also been proposed; when combined with giving preference to allocating peripheral submeshes it resulted in significant system performance improvements [4].

4.3.3 Reservation Best-Fit (RBF). In this scheme, proposed in [12], switching the orientation of requests is also allowed, and the goal of the allocation submesh selection scheme is to leave large free submeshes for future allocation, as was discussed earlier. Also, because our simulations have shown that the system performance of RBF depends on the order of *MFL* elements, we have ordered them as in [12] in the proposed *MFL* detection scheme when it was used with RBF so as to have the same performance as the original proposal.

5 Simulation Results

Simulation was employed for evaluating and comparing the maximal free submesh detection schemes when they were used with the three allocation submesh selection schemes considered. To this end, we implemented the detection and selection schemes in the ProcSimity simulator that we have been adding our proposed scheduling and allocation algorithms to for the last two decades. The original ProcSimity is a C-language tool that was developed initially at the University of Oregon for research in processor allocation and job scheduling for distributed memory multicomputers [21].

As in many previous related works, the 2D mesh system has equal sides of length L [1, 3, 6, 9, 12, 14, 26]. Job interarrival times follow an exponential distribution, and the scheduling algorithm assumed is first-come-first-served. Job execution times follow an exponential distribution with a mean of one time-unit. The side-lengths of allocation requests are generated using two distributions: the uniform over the interval $[1, L]$, and a uniform-decreasing distribution

that uses four probabilities pr_1, pr_2, pr_3 and pr_4, and four side lengths sl_1, sl_2, sl_3, and sl_4. These probabilities are for the α and β of a request to fall within [1, sl_1], [sl_1+1, sl_2], [sl_2+1, sl_3] and [sl_3+1, $s\ l_4$]. The side lengths within a range are distributed uniformly. In this paper, we use pr_1 = 0.4, $pr_2 = pr_3 = pr_4$ = 0.2, $sl_1 = L/8$, $sl_2 = L/4$, $sl_3 = L/2$, and $sl_4 = L$. The distributions adopted here were used in several previous research works [1, 3, 6, 9, 14, 15]. Independent simulation runs are repeated so as to have a 95% confidence level that relative errors do not exceed 5% of the means. In each simulation run, 1000 jobs are executed.

The system performance parameter measured in this study is the *average turnaround time* for all jobs, where a job's turnaround time is the time the job spends in the system. The efficiency of the detection schemes is evaluated using the time taken allocating and de-allocating. This second performance parameter is the main parameter because the two detection schemes are expected to produce *similar* system performance since they are both based on detecting the set of maximal free submeshes and are recognition-complete. In what follows, we denote the policies as <*D*>(<*S*>), where *D* is the detection scheme and *S* is the allocation submesh selection scheme. The proposed MFL detection scheme is denoted as PMFL, and that proposed by Kim and Yoon in [12] is denoted as KYMFL.

We first compare the system performance of the schemes for the workload models assumed. In Figure 8, the average turnaround times are plotted against average job arrival rates for the detection and allocation schemes and the uniform-decreasing size distribution in a 32 × 32 system. It can be seen in this figure that PMFL and KYMFL have, as expected, similar system performance. The results for the uniform distribution lead also to a similar conclusion, however they are not shown to conserve space. Also, simulations for other system sizes that grow to thousands of cores (16 × 16, 64 × 64, 128 × 128 and 256 × 256) do not modify this system performance conclusion for PMFL and KYMFL. The detection schemes PMFL and KYMFL have similar system performance because they both detect the unique set of maximal free submeshes. Also, MMPL and RBF have similar performance, and they outperform SFF substantially. Note that MMPL is a simpler scheme when compared with RBF.

To compare the policies in terms of allocation and de-allocation times, we measured the average actual times taken by the combination of these operations for five hundred runs of the simulator. In Figures 9 and 10, we show the. combined measured times against the job arrival rates under

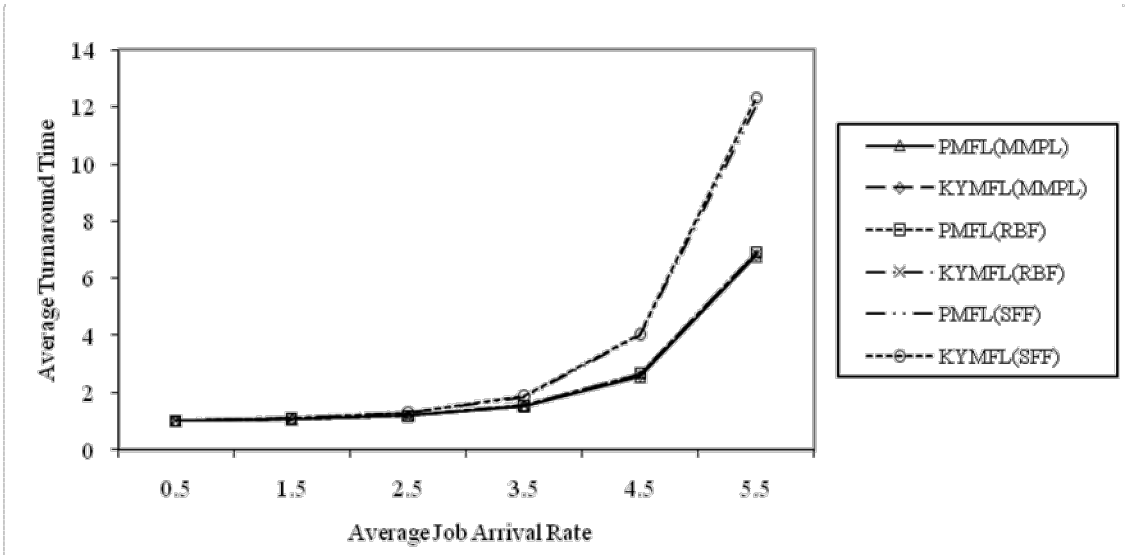


Figure 8: Average job turnaround times in a 32 × 32 system for the uniform-decreasing size distribution

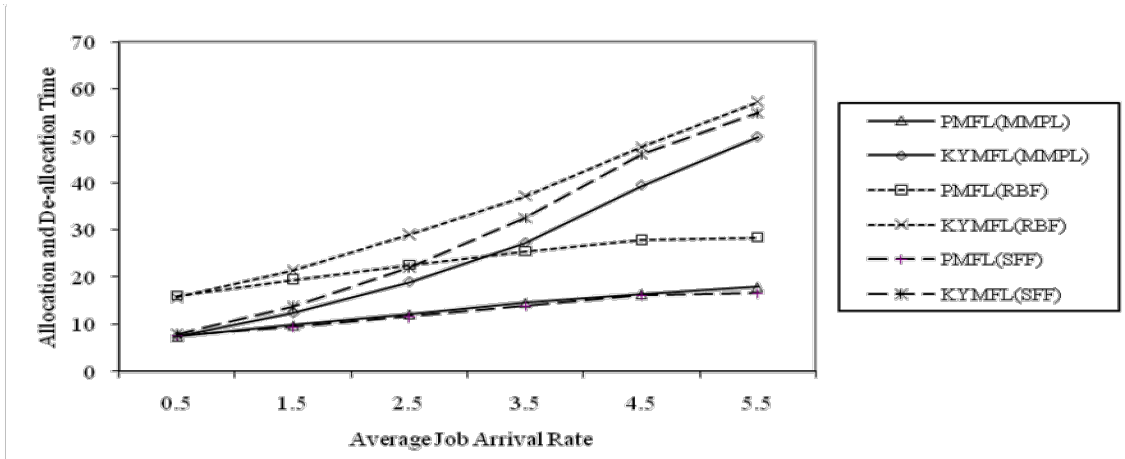


Figure 9: Measured combined times in a 32 × 32 system for the uniform-decreasing size distribution

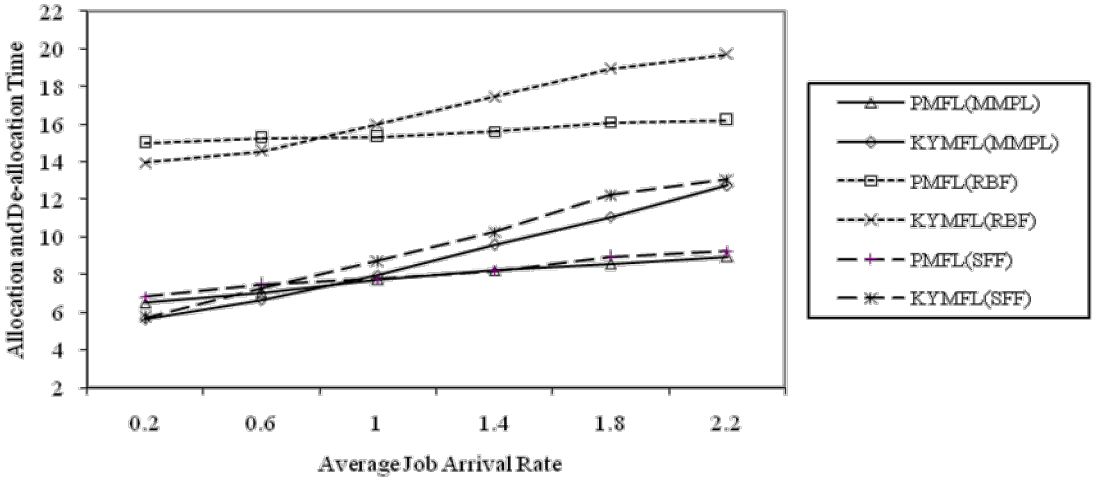


Figure 10: Measured combined times in a 32 × 32 system for the uniform size distribution

the size distributions considered in a 32 × 32 system. In these figures PMFL outperforms KYMFL substantially. Moreover, the advantage of PMFL is superior when the size distribution is uniform-decreasing. The reduction in the combined times for PMFL reaches 70% in Figure 9, and30% in Figure 10. Under the uniform-decreasing distribution, the average job size is smaller than under the uniform distribution, leading to a larger number of allocated (and free submeshes). This results in superior advantage for PMFL.

The average number of maximal free submeshes was computed for the simulations. This number increases with the system load and depends on the allocation scheme. As expected, it is comparatively small and varied from 1.16 to 3.22 for the uniform distribution. For the uniform-decreasing distribution, it varied from 1.5 to 9.85.

To illustrate the efficiency advantage of PMFL more clearly, we plot, in Figures 11 and 12, the relative measured times for PMFL with respect to KYMFL. In these figures, we have R(*S*) =T(PMFL(*S*))/T(KYMFL(*S*)), where T(PMFL(*S*)) is the measured simulation allocation and de-allocation time for PMFL when the selection algorithm is *S*, and T(KYMFL(*S*)) is this time for KYMFL and the same selection algorithm. Figure 11 shows that the efficiency advantage of PMFL over KYMFL is substantial under most loads. It increases with the load because the number of free submeshes, *f*, also increase with the load. The reduction in the combined times reaches about 50% for RBF, and it reaches about 70% for SFF and MMPL.

In Figure 12, the performance advantage of PMFL for medium to heavy loads is less substantial because *f* is smaller when the size distribution is uniform. The reduction in the combined times reaches about 10% for RBF, and it reaches about 30% for SFF and MMPL under heavy loads.

In summary, PMFL and KYMFL have similar system performance as they have identical submesh recognition capability, however PMFL can be much more time efficient than KYMFL, especially when the number of free submeshes is large. The numbers of allocated and free submeshes are larger when the core allocation requirements of jobs are small.

In Figure 13, we show the combined allocation and de-allocation times of the detection and selection policies for various side lengths under the system load of 4.5 jobs/time unit and the uniform-decreasing side-length distribution. Figure 14 is for a load of 1.8 jobs/time unit and the uniform

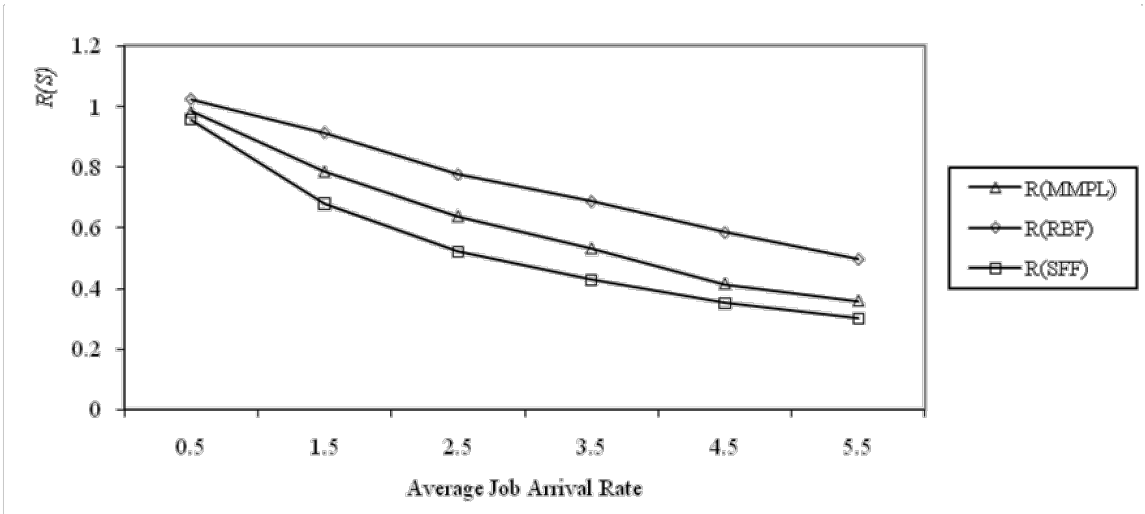


Figure 11: Ratio of the measured times for the allocation submesh selection policies and the uniform-decreasing size distribution in a 32 × 32 system

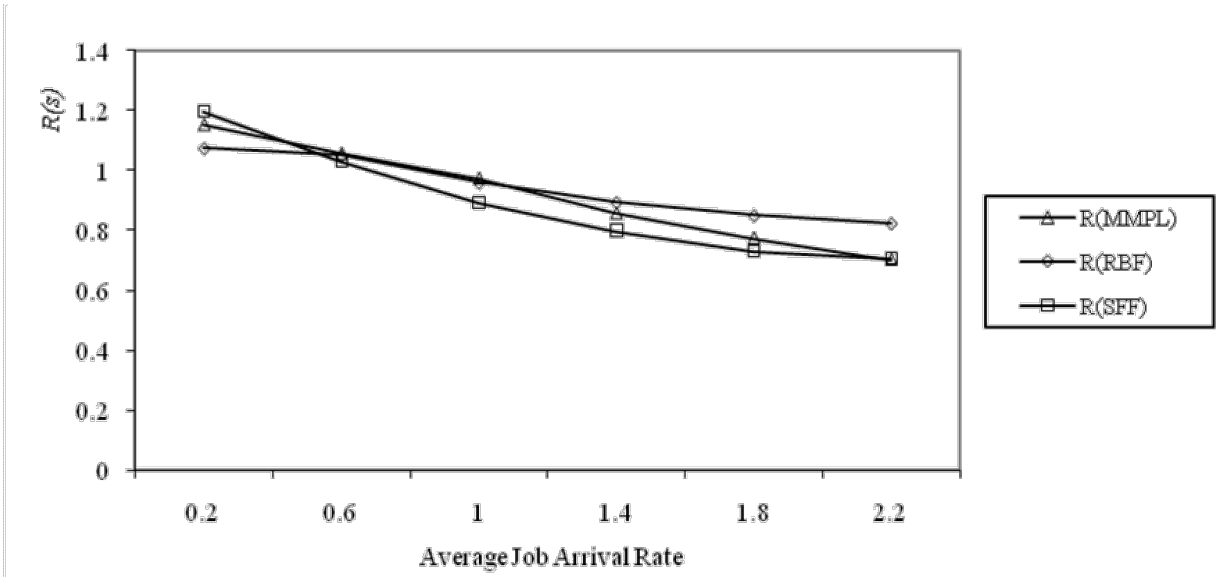


Figure 12: Ratio of the measured times for the allocation submesh selection policies and the uniform size distribution in a 32 × 32 system

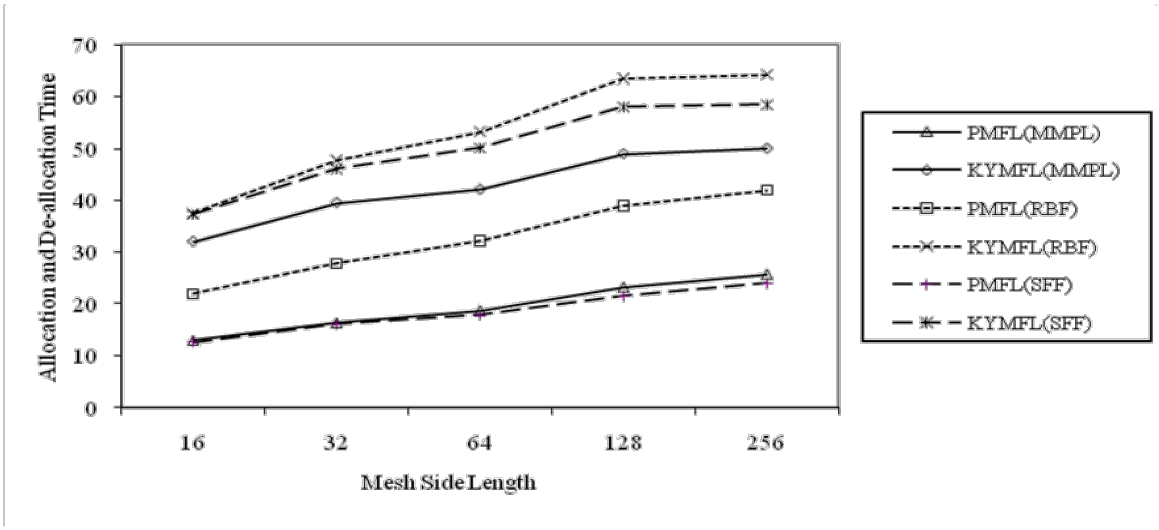


Figure 13: Measured combined times for doubled side lengths under the uniform-decreasing size distribution and a system load of 4.5 jobs/time unit

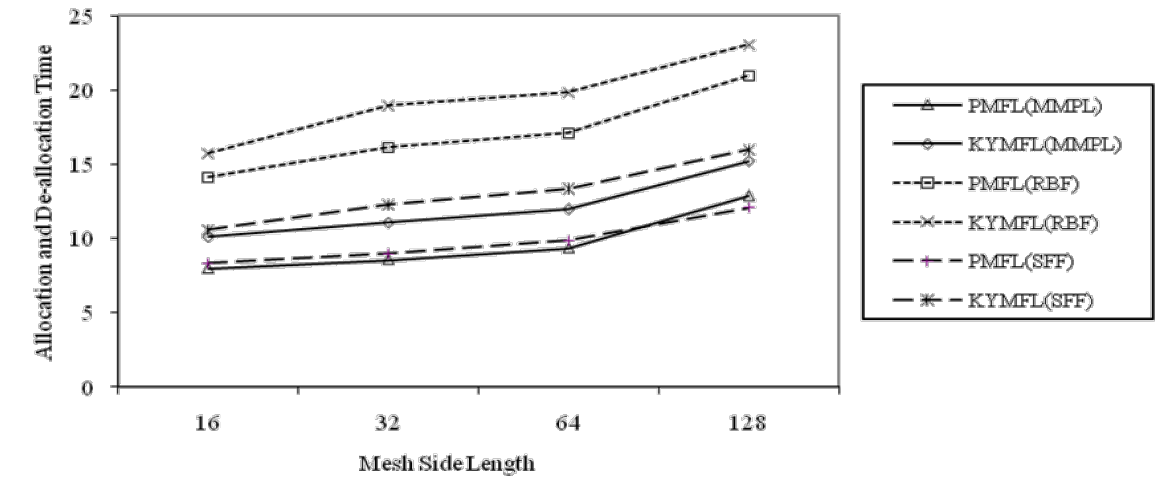


Figure 14: Measured combined times for doubled side lengths under the uniform size distribution and a system load of 1.8 jobs/time unit

performance advantage of PMFL can remain substantial as the size of the computer system grows to tens of thousands of cores.

6 Conclusions

In this paper, we have proposed an efficient maximal free submesh detection scheme for space-sharing allocation in manycore systems with 2D NoCs. Several studies indicate that space-sharing is a promising core allocation strategy in manycore systems, as it can achieve scalability and good performance for large core numbers [22, 25]. Parallel jobs or applications, including the OS, run on their own sets of cores, which can reduce interference among jobs, message delays, energy consumption and chip temperatures. Studies have shown that mapping the communicating tasks of a parallel job to neighboring cores, in particular those forming a submesh, can reduce communication delays and power consumption, and improve throughput and job execution times [5, 8, 18]. In this research, maximal free submeshes that are not contained in other free submeshes are detected and placed in a free-list. An advantage of this scheme over that proposed previously is that its time complexity is quadratic in *f*, whereas that of the previous scheme is cubic in this number. In addition to this theoretical comparison, the two recognition-complete detection schemes were evaluated and compared using detailed simulations when three promising allocation submesh selection schemes were used in combination with these detection schemes. The results show that the detection schemes have similar free submesh recognition-capability and average turnaround times, however the proposed scheme is overall substantially more efficient than the previous scheme in terms of the combined allocation and de-allocation times. Also, the simulated time performance advantage increases with the number of free submeshses, which is compatible with the time complexity advantage. It is to be noted that detecting maximal free submeshes is suitable for achieving simple, flexible, and efficient selection of allocation submeshes as the largest free submeshes are readily available in a list. The results also show that the simple scheme MMPL achieves good system performance. It outperforms SFF and achieves similar performance to the more complicated RBF scheme. As extensions to this work, more general defragmentation algorithms that make use of the efficient MFL detection mechanisms proposed in this work could be investigated.

Acknowledgment

We would like to thank Al al-Bayt University as this research has been carried out during a sabbatical leave for Ismail Ababneh.

References

[1] I. Ababneh, "An Efficient Free-List Submesh Allocation Scheme for Two-Dimensional Mesh-Connected Multicomputers," *Journal of Systems and Software*, 79:1168-1179, 2006.

[2] I. Ababneh, "A Performance Comparison of Contiguous Allocation Placement Schemes for 2D Mesh-Connected Multicomputers," 2007 ACS/IEEE International Conference on Computer Systems and Applications, (AICCSA 2007), Amman, Jordan, May 13-16, 2007.

[3] I. Ababneh, "On Submesh Allocation for 2D Mesh Multicomputers using the Free-List Approach: Global Placement Schemes," *Performance Evaluation*, 66(2):105-120, 2009.

[4] I. Ababneh, S. Bani-Mohammad, and M. Ould-Khaoua, "All Shapes Contiguous Submesh Allocation for 2D Mesh Multicomputers," *International Journal of Parallel, Emergent, and Distributed Systems,* 25(5):411-421, 2010.

[5] M. O. Agyeman, A. Ahmadinia, and N. Bagherzadeh, "Energy and Performance-Aware Application Mapping for Inhomogeneous 3D Networks-on-Chip," *Journal of Systems Architecture*, 89:103-117, September 2018.

[6] G.-M. Chiu and S.-K. Chen, "An Efficient Submesh Allocation Scheme for Two-Dimensional Meshes with Little Overhead," *IEEE Trans. on Parallel and Distributed Systems*, 10(5):471-486, 1999.

[7] P.-J. Chuang and N.-F. Tzeng, "Allocating Precise Submeshes in Mesh Connected Systems," *IEEE Trans. on Parallel and Distributed Systems*, 5(2):211-217, 1994.

[8] N. Dahir, A. Karkar, M. Palesi, T. Mak, and A. Yakovlev, "Power Density Aware Application Mapping in Mesh-Based Network-on-Chip Architecture: An Evolutionary Multi-Objective Approach," *Integration*, 81:342-353, November 2021.

[9] D. Das Sharma and D. K. Pradhan, "Submesh Allocation in Mesh Multicomputers using Busy-List: A Best-Fit Approach with Complete Recognition Capability," *J. of Parallel and Distributed Computing*, 36:106-118, 1996.

[10] J. Ding and L.-N. Bhuyan, "An Adaptive Submesh Allocation Strategy for Two-Dimensional Mesh Connected Systems," *Proc. Int'l Conf. Parallel Processing II*, pp. 193-200,1993.

[11] P. Gratz, C. Kim, K. Sankaralingam, H. Hanson, P. Shivakumar, S. W. Keckler, and D. Burger, "On-Chip Interconnection Networks of the TRIPS Chip," *IEEE Micro*, 27(5):41-50, November 2007.

[12] G. Kim and H. Yoon, "On Submesh Allocation for Mesh Multicomputers: A Best-Fit Allocation and a Virtual Submesh Allocation for Faulty Meshes," *IEEE Trans. on Parallel and Distributed Systems*, 9(2):175-185, 1998.

[13] H. Lahdhiri, J. Lorandel, S. Monteleone, E. Bourdel, and M. Palesi, "Framework for Design Exploration and Performance Analysis of RF-NoC Manycore Architecture," *Journal of Low Power Electronics and Applications*, 10(4):37, MDPI 2020.

[14] T. Liu, W.-K. Huang, F. Lombardi and L. N. Bhuyan, "A Submesh Allocation Scheme for Mesh-Connected Multiprocessor Systems," *Proc. Int'l Conf. Parallel Processing II*, pp. 159-163,1995.

[15] V. Lo, K. J. Windisch, W. Liu, and B. Nitzberg, "Noncontiguous Processor Allocation Algorithms for Mesh-Connected Mutlicomputers," *IEEE Trans.*

on Parallel and Distributed Systems, 8(7):712-725, 1997.

[16] H. Matsutani, M. Koibuchi, and H. Amano, "Tightly-Coupled Multi-Layer Topologies for 3-D NoCs," 2007 International Conference on Parallel Processing, ICPP [4343882], *Proceedings of the International Conference on Parallel Processing*, pp. 75-85, https://doi.org/10.1109/ICPP.2007.79, 2007

[17] S. Mazumdar and A. Scionti, "Ring-Mesh: A Scalable and High-Performance Approach for Manycore Accelerators," *The Journal of Supercomputing*, 76:6720-6752, 2020.

[18] A. Mosayyebzadeh, M. M. Amiraski, and S. Hessabi, "Thermal and Power Aware Task Mapping on 3D Network on Chip," *Computers and Electrical Engineering*, 51:157-167, April 2016

[19] J. Ng, X. Wang, A. Singh, and T. Mak, "Defragmentation for Efficient Runtime Resource Management in NoC-Based Many-Core Systems," *IEEE Trans. on Very Large Scale Integration (VLSI) Systems*, 24(11):3359-3372, 2016

[20] A. Pathania, V. Venkataramani, M. Shafique, T. Mitra, and J. Henkel, "Defragmentation of Tasks in Many-Core Architecture," *ACM Trans. on Architecture and Code Optimization*, 14(1):1-21, 2017

[21] ProcSimity, *ProcSimity v4.3 User's Manual*, University of Oregon, May 17, 1996.

[22] H. Sasaki, T. Tanimoto, K. Inoue, and H. Nakamura, "Scalability-Based Manycore Partitioning," PACT'12, Minneapolis, Minnesota, USA, September 19-23, 2012.

[23] S. Vangal, J. Howard, G. Ruhl, S. Dighe, H. Wilson, J. Tschanz, D. Finan, P. Lyer, A. Singh, T. Jacob, S. Jain, S. Venkataraman, Y. Hoskote, and N. Borkar, "An 80-Tile 1.28TFLOPS Network-on-Chip in 65nm CMOS," *2007 IEEE International Solid-State Circuits Conference. Digest of Technical Papers*, pp. 98-589, doi: 10.1109/ISSCC.2007.373606, 2007.

[24] D. Wentzlaff, P. Griffin, H. Hoffmann, B. Liewei, B. Edwards, C. Ramey, M. Mattina, M. Chyi-Chang, J.F. Brown, and A. Agarwal, "On-Chip Interconnection Architecture of the Tile Processor," *Micro, IEEE*, 27(5):15-31, November 2007

[25] D. Wentzlaff, C. Gruenwald, N. Beckmann, K. Modzelewski, A. Belay, L. Youseff, J. Miller, and A. Agrawal, "A Unified Operating System for Clouds and Manycore: fos," Computer Science and Artificial Intelligence Lab, MIT, Tech. Rep. MIT-CSAIL-TR-2009-059, Nov. 2009

[26] S.-M. Yoo, H. Y. Youn, and B. Shirazi, "An Efficient Task Allocation Scheme for 2D Mesh Architectures," *IEEE Trans. on Parallel and Distributed Systems*, 8(9):934-942, 1997.

[27] Y. Zhu, "Efficient Processor Allocation Strategies for Mesh-Connected Parallel Computers," *J. Parallel and Distributed Computing*, 16:328-337, 1992.

[28] X. Zhu and W.-M. Lin, "Allocation-Time-Based Processor Allocation Scheme for 2D Mesh Architecture," *J. of Information Science and Engineering*, 16:301-311, 2000.

Ismail Ababneh received a BS degree in Electromechanical Engineering from the National Superior School of Electronics and Electro-mechanics of Caen, France, in 1979, the MS degree in Software Engineering from Boston University in 1984, and the Ph.D. degree in Computer Engineering from Iowa State University in 1995. From 1984 to 1989, he was a Software Engineer with Data Acquisition Systems, Boston, Massachusetts. He is presently a professor in the Department of Computer Science at Al al-Bayt University in Jordan. From 2007 to 2010, he was a visiting associate professor in the Department of Computer Science at Jordan University of Science and Technology. He is a member of Tau Beta Pi and Eta Kappa Nu. He held several administative positions at Al al-Bayt University, including Head of Computer Science Department, Dean of IT College, Director of Computer Center, Dean of Research, and Vice President for Administration and Student Affairs. His current research interests include processor allocation in multicomputers, and ad hoc routing algorithms. He has published about 70 papers in journals, conferences and workshops.

Saad Bani-Mohammad received the BSc degree in computer science from Yarmouk University, Jordan in 1994, the MSc degree in computer science from Al al-Bayt university, Jordan in 2002, and the PhD degree in computer science from University of Glasgow, U.K., in 2008. From 2002 to 2005, he was a lecturer in the Department of Computer Science at Al al-Bayt University in Jordan. Prof. Bani-Mohammad served as a Head of Computer Science Department for 5 years (2008-2013) at Al al-Bayt University, and a Deputy Dean of the IT College at Al al-Bayt University for one year (2013-2014), and then he served as a Dean of Prince Hussein Bin Abdullah College for Information Technology at Al al-Bayt University for 6 years (2015-2020). Prof. Bani-Mohammad is presently a President's Assistant of Accreditation and Quality Assurance Commission for Higher Education Institutions (AQACHEI) in Jordan and a Professor of Computer Science in the Department of Computer Science at Al al-Bayt University, Jordan. He is a member of IEEE Computer Society. His research interests include processor allocation and job scheduling in multicomputers and E-learning. Prof. Bani-Mohammad has over 40 scientific papers and projects either presented or published. Most of his research was supported by Al al-Bayt University, Jordan and University of Glasgow, U.K. His findings were published (over 40 publications) in world leading journals and also in prestigious and top quality international conference proceedings.

The Combination of Ontology-Driven Conceptual Modeling and Ontology Matching for Building Domain Ontologies: E-Government Case Study

Shaimaa Haridy*, Rasha M. Ismail*, Nagwa Badr*, and Mohamed Hashem*
Ain Shams University, Cairo, Egypt

Abstract

During the last decade, ontology engineering has undoubtedly participated in a lot of beneficial applications in different domains. Nevertheless, ontology development still faces several significant challenges that need to be addressed. This study proposes an enhanced architecture for the ontology development lifecycle. With the help of this architecture, users can complete ontology development tasks since it provides guidance for all key activities, from requirement specification to ontology evaluation. Ontology-driven conceptual modeling (ODCM) and ontology matching serve as the foundation of this architecture. ODCM is defined as the application of ontological ideas from various fields to build engineering objects that improve conceptual modeling. Ontology matching is a promising approach to overcome the semantic heterogeneity challenge between different ontologies. The proposed architecture is applied to e-governance domain, which is one of the online services that gains a great attention worldwide, especially during the coronavirus pandemic. However, residents of Arab countries face numerous obstacles and do not receive the full benefits of e-governance. For these reasons, Egyptian e-government is selected as the suggested case study. The results are encouraging when the produced ontology is compared with 20 existing ontologies from the same domain. On the basis of OntoMetrics, the average values of metrics correlated to accuracy, understandability, cohesion and conciseness lie in the 95th, 95th, 95th and 57th percentiles respectively. The results can be further enhanced by defining more non-inheritance relations and distributing the instances across all classes.

Key Words: Artificial intelligence, digital government (e-government), ontology-driven conceptual modeling, ontology engineering, ontology enrichment, ontology matching, OntoUML, semantic web.

1 Introduction

In recent years the enormous growth of semantic web theories and techniques facilitates using ontologies extensively in numerous domains and applications [2]. Authors in [16] defined ontology engineering as "The set of activities that concern the ontology development process, the ontology life cycle, and the methodologies, tools and languages for building ontologies". It seeks to provide standard components for creating knowledge models. Conceptualization is one of the crucial activities in ontology engineering. Conceptualization focuses on recognizing the concepts in the real world to build the model of the relevant domain [40]. This activity has a significant impact on the quality of the final ontology, as the quality of any artifact based on a model is constrained by the model's quality [21]. Researchers proposed a new method known as ontology-driven conceptual modeling (ODCM) [13] that greatly aid in ontology conceptualization. ODCM is described as the application of ontological ideas from various fields, such as formal ontology, cognitive science, and philosophical logics, to build engineering objects that improve conceptual modeling theory and practice. One of the most used languages in ODCM is OntoUML [13], which is "a language whose meta-model has been designed to comply with the ontological distinctions and axiomatization of a theoretically well-grounded foundational ontology named UFO (Unified Foundational Ontology)" [20]. UFO is "an axiomatic formal theory based on contributions from Formal Ontology in Philosophy, Philosophical Logics, Cognitive Psychology, and Linguistics" [22].

Ontology engineering has undoubtedly participated in a lot of beneficial applications in the last decade, but there are still significant challenges about ontology development that need to be solved [34]. One of the challenges that face ontology-based applications is ontology heterogeneity which emerges from varying expertise of knowledge engineers who create and maintain ontologies in the same domain. For that reason, ontology matching is widely used in ontology engineering to solve this heterogeneity problem [25].

The digital government or electronic government (e-government) is one of the critical domains that could benefit from ontology engineering. It provides public services to citizens solely by means of information and communication technologies, such as computers and Internet [45]. However, the residents of Arab countries have faced numerous obstacles and have not received the full benefits of e-governance. Egypt's Ministry of Communications and Information Technology, in collaboration with the Ministry

* Faculty of Computer and Information Sciences. Email: shaimaaharidy@cis.asu.edu.eg, rashaismail@cis.asu.edu.eg, nagwabadr@cis.asu.edu.eg, mhashem100@yahoo.com.

of State for Administrative Development, launched an e-government project. The first stage lasted from 2001 to 2007, and the second stage was from 2007 to 2012 [18]. Nevertheless, in 2020, the United Nations ranked Egypt as 111th out of 193 nations in terms of using e-government to provide public services; and the ninth in the Arab world [41]. This is due to the numerous obstacles faced in the growth of e-government [18]. Some of these challenges are:

1) There are no standards or specifications, which makes it difficult for government entities to communicate and integrate.
2) The government agencies are not able to share information that prohibits them from performing e-government efforts properly and effectively.
3) There is no unified standard for repeated inquiries made by citizens to the various government agencies.

Consequently, the goal of this research is to present an enhanced ontology engineering architecture for building domain ontologies from scratch. ODCM and ontology matching serve as the foundation of the proposed architecture. The e-government domain in Egypt is selected as the case study. The three main contributions of this study are: (1) the combination of ODCM conceptual modeling with ontology matching, (2) two new algorithms for the selection of the most relevant ontology and the extraction of new classes and relations, as well as (3) the new domain ontology for the Egyptian e-government. The remainder of the paper is organized as follows. Section 2 gives a review of the related work. A description of the proposed architecture is offered in Section 3. Section 4 discusses the results of the experiments. Finally, Section 5 states the conclusions and future work.

2 Related Work

There has been a tremendous amount of work proposed in the literature to cover various ontology-related aspects and their application in diverse disciplines. Some recent studies related to ontology-driven conceptual modeling, ontology matching, and e-government will be discussed in the following subsections.

2.1 Ontology-Driven Conceptual Modeling

The papers in this context are divided into two categories. OntoUML was used by the first group due of its widespread use in crucial and complex sectors, such as [2, 8-10, 17, 22, 36]. Whereas the second used alternative languages, like [1, 5, 26, 35, 39]. Table 1 provides a summary of the work done by these prior studies. Despite OntoUML's success in other domains, it has not yet been applied in e-government.

A. 2.2 Ontology Matching

The ontology matching task has been discussed for a decade. For example, authors in [42] acquired knowledge from groupware using facts enrichment approach (FEA). The advantage of this approach resides in its capacity to extract new concepts from unstructured text and insert those new concepts into an already-existing ontology. In [4], researchers improved the ontology matching task by merging several alignments generated by different matchers. Their approach used background knowledge (BK) resources to drive paths between source and target ontologies. Finally, they proposed a selection algorithm in order to determine the final mapping. In [23] used ontology matching to improve emotion detection from text. The ontology of the input statement was matched with emotion labeled ontology base, and the emotion with the highest matching score was selected. Matching ontologies algorithm were developed in [3]. The goal of this algorithm was to match entities and sub-entities in the Ontology document with sentences that have the same topic. Ontology matching and ODCM each have advantages that have been discussed in the literature, but little has been written on how to combine the two to promote ontology engineering.

2.3 E-Government

For years, many efforts have been undertaken to overcome the barriers related to e-governance. Authors of [6] addressed some variables affecting the adoption of cloud computing in government organizations, because Saudi Arabian government recognized the benefits of cloud computing and tried to create basic protocols for delivering government services via the cloud. As for [18] and [44], both conducted research on Egypt's e-government and its challenges. In addition, they proposed remedies for these problems. In [18] the researchers achieved some progress, but more needs to be done to address the problems faced in the development of e-government. Moreover, Egypt is still behind a few Arab countries in delivering online information and providing government services. In [44], the authors stated that the Egyptian information technology sector was impacted by the political turmoil in recent years. Egypt's e-government development index was downgraded from high to medium in the global rankings. Its position plummeted 28 places from the 80th place in 2014 to the 108th place in 2016. In [27], the researchers demonstrated how semantic technology is critical for the development of e-government services. Semantic web services and ontologies allow the automated processing of services and information and improve communication between the parties involved. They examined a set of available information, standards, existing referenced models and certain semantic web service formalisms. In addition, a knowledge-based modeling framework for Moroccan e-government services and its implementations of e-customs was suggested.

Since literature review reveals that Egypt's e-government area lacks an ontology, it is chosen as the suggested case study in this paper.

Table 1: Summary of ODCM utilization in various domains

Reference	Language / Tool	Conceptual Model	Ontology	Detailed Steps	Detailed Evaluation	Literature Review	Domain
[17]	OntoUML	✓		✓		✓	Human Genome
[8]	OntoUML	✓	✓	✓	✓	✓	Railway
[33]	OntoUML	✓		✓		✓	Economic Exchanges
[10]	OntoUML		✓	✓	✓		Marketplace
[9]	OntoUML	✓	✓	✓			Marketplace
[35]	-	✓	✓	✓			Farm
[26]	CoreWEB	✓					Enterprise Information Systems
[39]	Protégé	✓	✓			✓	Cybersecurity Vulnerability
[2]	Menthor & E-OntoUML & StarUML	✓	✓	✓		✓	Agriculture
[5]	-	✓	✓	✓			Transmedia Storytelling
[1]	Protégé	✓	✓	✓	✓	✓	Human Affective States
[36]	OntoUML	✓	✓	✓		✓	Higher Education

3 Proposed Architecture

This study introduces an enhanced architecture for the ontology development lifecycle. With the help of this architecture, users can complete ontology development tasks since it provides guidance for all key activities, from requirement specification to ontology evaluation. The domain of e-governance in Egypt is the suggested case study. Figure 1 depicts the proposed architecture, which is composed of four main modules that are thoroughly detailed in the following subsections.

3.1 Requirement Specification Module

This module seeks to provide the ontology's prospective uses. This can be accomplished by reviewing available domain documents in their various formats, in addition to related online resources. The output of this module is the use case diagram. UML (Unified Modeling Language) design tools are helpful for this. The diagram helps in the comprehension of system functionalities, the elimination of function redundancies, and the review of relationships between different actors and system functions.

In the proposed case study, due to the shortage of documents describing the Egyptian e-government in detail, the Egyptian web portal [11] serves as the lone source of information to establish system requirements. The portal connects 14 consumers with 30 service providers. The citizen is the main consumer who uses the greatest number of services through the portal. This paper focuses on the citizen module, which includes 35 different services. Their use cases are presented using the Rational Rose tool [7].

3.2 Ontology Development Module

Although there is no universal consensus on the technique that can be considered ideal for ontology development, the goal of creating an ontology might help select the optimal methodology. METHONTOLOGY is an ontology-building methodology that specifies the life cycle of the ontology development process. The full explanation of the conceptualization activity, which is the focus of this work, is the key strength of this methodology [15]. Therefore, it is followed in the ontology development module in the proposed architecture. This module accepts as input the use case diagram generated from the preceding module, as well as domain documents, online resources, and existing ontologies. As for output, a new domain ontology is produced. Subsequently subsections provide description of ontology development activities.

A written document in natural language is used to describe the ontology information in this activity. A common proposal for describing ontologies is the ontology metadata vocabulary (OMV). It allows for easy access to and exchange of ontologies across the Internet [24]. The OMV of the suggested ontology is given above.

The NeOn methodology [37] provides versatile possibilities for the reuse and re-engineering of knowledge sources for developing ontology networks. The following three scenarios are used by proposed ontology:

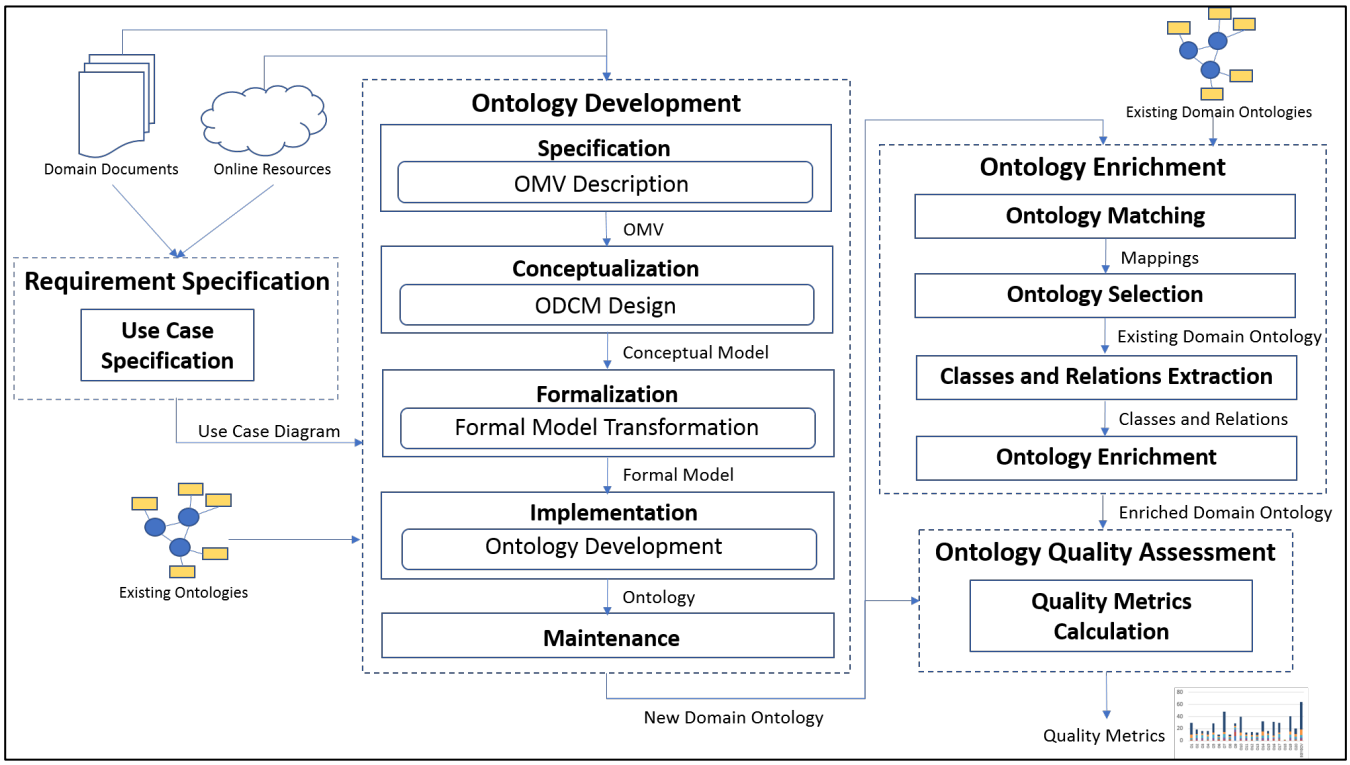


Figure 1: Proposed architecture

3.2.1 Specification

Egyptian E-government Ontology Metadata Vocabulary OMV
Ontology Name: Egyptian E-government Ontology (EGYGOV)
Location: Ain Shams University, Cairo, Egypt
Party (Organization): Ain Shams University
License Model: Academic research
Ontology Type: Domain Ontology
Ontology Domain: Electronic government (e-government)
Ontology Engineering Tool: OntoUML Lightweight Editor (OLED)
Ontology Language: OWL
Ontology Syntax: rdf xml Syntax
Ontology Task: Describes data and services of Egyptian e-government. EGYGOV represents a model for the semantic description of governmental features such as domain concepts, services, regulations, and organizational structures.
Ontology Engineering Methodology: NeOn Methodology for Building Ontology Networks; EGYGOV follows different scenarios:
Scenario 1: From specification to implementation.
Scenario 2: Reusing and re-engineering non-ontological resources.
Scenario 3: Reusing and re-engineering ontological resources.
Source of Knowledge: Non ontological resources (Egyptian e-government portal), Ontological resources (existing ontologies)

- Scenario 1: From specification to implementation. The ontology is developed from scratch.
- Scenario 2: Reusing and re-engineering non ontological resources. Egyptian e-government portal [11] is the non-ontological resource used to build the ontology. Re-engineering entails transferring this resource to an ontology format and possibly modifying the class name.
- Scenario 3: Reusing and re-engineering ontological resources. EGYGOV reused UFO-S [31], which is a core reference ontology that captures a clear account of services and service-related concepts.

3.2.2 Conceptualization. A model of the relevant domain knowledge is built in this step. This model can take any shape that domain experts accept and understand [15]. The proposed conceptual model is implemented using OLED [19], which is a model-based environment for

formalizing, implementing, testing, and validating OntoUML models. Class and relationship stereotypes of OntoUML are described in depth in [38].

Two alternative portions of the designed conceptual model are shown in Figures 2 and 3. In Figure 2, the *Service Delivery* class consists of *Request* of the consumer, *Response* of the provider, *Description, Conditions* to be accepted, and *Actions* to be performed; as well as *Documents* to be extracted. For *Service Delivery*, two options are possible: *Free* or *Paid*. The *Request* has three possibilities: *Pending*, *Processed*, or *Cancelled*. The *Agent* category includes *Provider* and *Consumer*; *Provider* has many *Entities* and each one has a *Location*. Note that *Service*, *Agent*, *Provider*, and *Consumer* are reused and reengineered from the UFO-S core ontology. Figure 3 displays a portion of the *Citizen* class and *Violations* on his *Vehicle License* and *Driving License*. Both licenses are generalized from the *License* class. *Phone Line* has *Mobile Line* and *Land Line* as its descendants. Also, the citizen makes a *Phone Subscription* to his *Phone Line* which is associated with a *Phone Bill, a*s well as, the *Electricity Subscription* made to an *Electricity Meter* with its *Consumption Readout* and *Complaints* and *Inquiries* made by citizens.

3.2.3 Formalization. The aim of this activity is to output a model in an implementation language. Therefore, the preceding activity's well-founded conceptual model is transformed into a formal model using OLED code generation feature. As a result, the proposed model is converted from OntoUML model to OWL ontology.

3.2.4 Implementation. Using the protégé tool [309] the resulting OWL ontology is enhanced with data properties and individuals (instances), as displayed in Figures 4 and 5, respectively. For example, properties such as IDs, Texts are added to Condition, Complaint and Area classes. Dates are added to Birth Certificate, Document and Consumption Readout classes. Description is added to Service class.

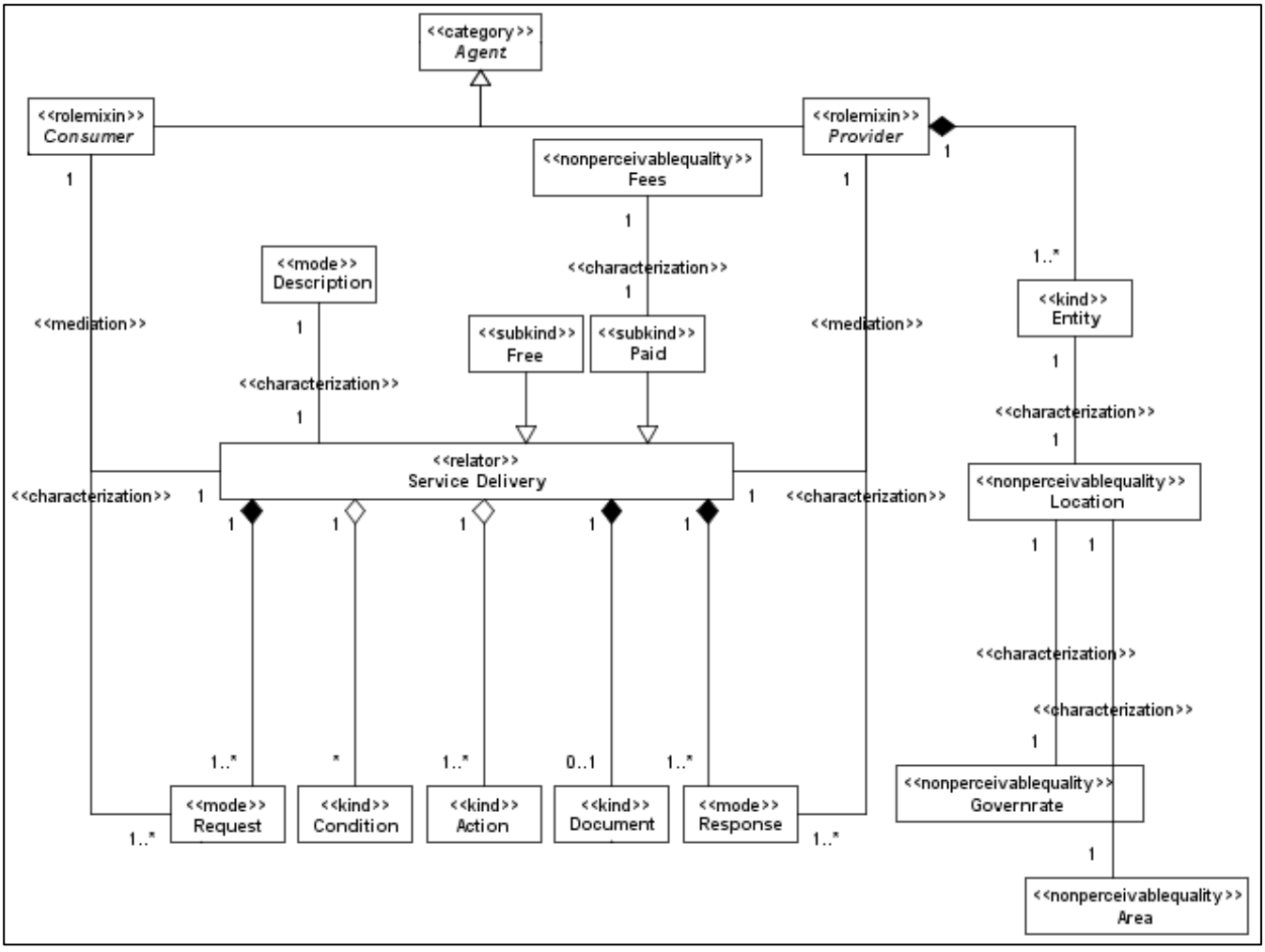


Figure 2: A fragment of the proposed conceptual model: The service delivery class

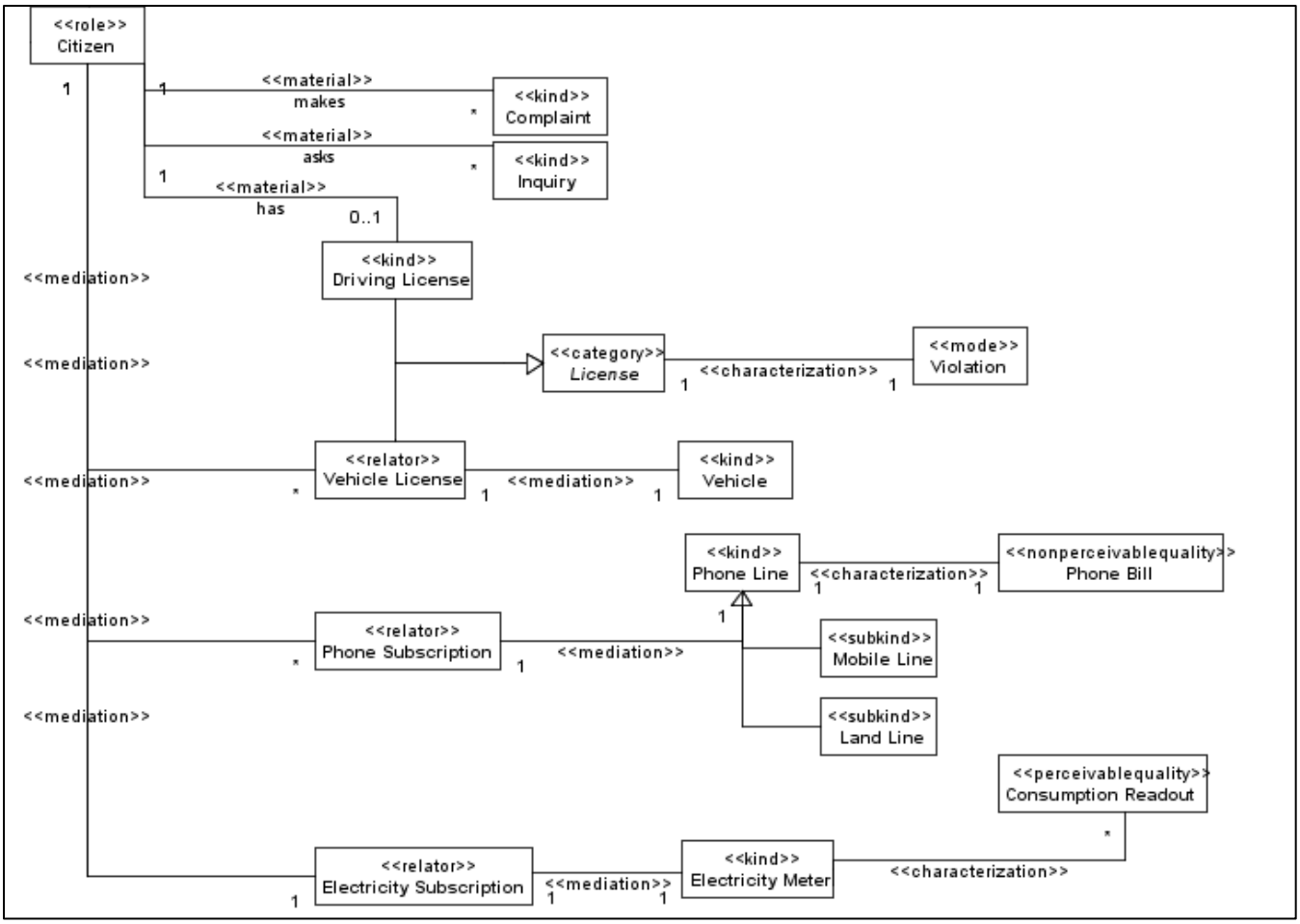


Figure 3: A fragment of the proposed conceptual model: The citizen class *documents*

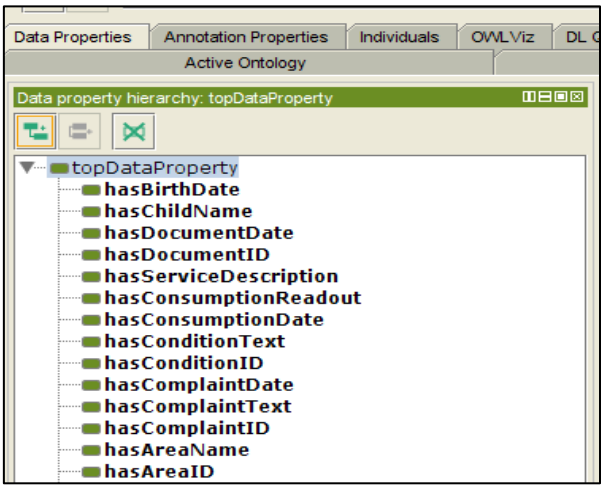


Figure 4: A fragment of data properties

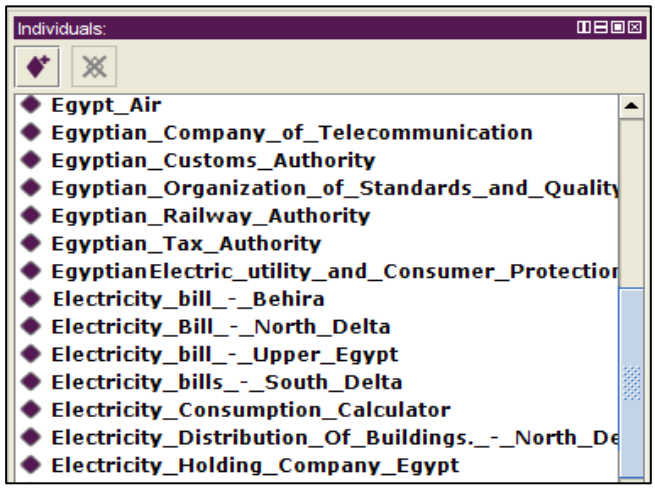


Figure 5: A fragment of individuals

Individuals are defined to classes such as *Ministry*, *Company, Authority, Office*, *Organization, Governorate* and *Request*.

3.2.5 Maintenance. This activity involves making any necessary updates or corrections to the ontology.

3.3 Ontology Enrichment Module

The ontology enrichment seeks to evolve their semantic content in order to cover new knowledge and enhance their semantic consistency 12]. In the current module, this is accomplished by finding new concepts and relations, then inserting them into the ontology. Although this new knowledge can come from a variety of sources, the existing domain ontologies are the main focus of this article. This enables the integration of domain knowledge from different perspectives. This module receives as input a set of existing domain ontologies in addition to the ontology created in the previous module. The output is an enriched domain ontology. This module consists of four activities described below. The paper proposes two novel algorithms. Algorithm 1 for the selection of the most relevant domain ontology, and Algorithm 2 for the extraction of relevant classes and relations.

3.3.1 Ontology Matching. This activity identifies correspondences between proposed ontology's entities and those in already existing domain ontologies. This can be accomplished by using one of the available matchers. AML [32] is one of the most effective matching systems. It has the advantage of the data structures generated for its word matcher. When an ontology is loaded, it builds a new lexicon with all class labels and synonyms using a bag-of-words technique. Additionally, a relationship map [13] data structure is created, which connects each class to the classes related to it via a part of relationships or disjoint clauses. In the domain of e-government, data of 20 existing ontologies were collected in the paper [14]. Unfortunately, only ten of them are accessible for download. So, in this case study AML matcher is used along with some customized code to match the proposed ontology with those ten ontologies. Therefore, results of their generated data structures (lexicon and relationship map) are displayed in Table 2. The output of this activity is mappings between the proposed ontology (EGYGOV) and each of the ten domain ontologies.

3.3.2 Ontology Selection. Based on the mappings produced by the previous activity, the most pertinent domain ontology is selected. one with the greatest number of mappings to the proposed ontology (EGYGOV). It is O_{18} as shown in Table 3.

3.3.3 Classes and Relations Extraction. The aim of this activity is to extract the list of classes and relations that will be injected later in the proposed ontology. To do this, there are two key steps: first, find the classes that exist in the mappings of the most relevant ontology and then look for the relationships of each class within the domain ontology itself. In this case the output list contains 748 classes and 1456 relationships.

3.3.4 Ontology Enrichment. This activity is the last step in the enriching process in which classes and relationships are inserted into the proposed ontology. To eliminate duplications or inappropriate insertions, the extracted list must first undergo a comprehensive editing. The list is thereby condensed to 703 classes and 830 relationships. They are injected in the proposed ontology using the protégé tool [30], then data properties and individuals for those new classes need to be defined.

Algorithm 1 - The Most Relevant Domain Ontology Selection

```
INPUT: Proposed ontology (proposedonto)

INPUT: List of existing domain ontologies
(domainontolist)

OUTPUT: The most relevant domain ontology and
its mappings with the proposed ontology

BEGIN
1    SET maxmappcnt TO 0
    //ONTOLOGY MATCHING
2    LOAD proposedonto INTO sourceonto
3    FOR EACH onto IN domainontolist DO
4      LOAD onto INTO targetonto
5      CONSTRUCT ONTOLOGY OBJECTS
6      BUILD LEXICON
7      BUILD RELATIONSHIP MAP
8      mappings ← ALIGN ONTOLOGY OBJECTS
      //ONTOLOGY SELECTION
9      IF mappings.count > maxmappcnt THEN
10       SET maxmappcnt To mappings.count
11       SET mostrelvonto TO targetonto
12       SET mostrelvmapps TO mappings
13     END IF
14   END FOR
15   RETURN (mostrelvonto, mostrelvmapps)
END
```

Algorithm 2 – The Relevant Classes and Relations Extraction

```
INPUT: The most relevant domain ontology
(mostrelvonto)

INPUT: The mappings between the proposed
ontology with the most relevant domain ontology
(mostrelvmapps)

OUTPUT: List of relevant classes and relations

BEGIN

1       FOR EACH mapp IN mostrelvmapps DO

2         class1id ← mapp.TARGETCLASSID

3         class1name ←
          mostrelvonto.GETCLASSNAME(class1id)

4         rels ←
          mostrelvonto.GETRELATIONS(class1id)

5         FOR EACH r IN rels DO

6           relname ← r.GETRELNAME()

7           class2id ← r.GETCLASS2ID()

8           class2name ←
            mostrelvonto.GETCLASSNAME(class2id)

9           outputlist.ADD (class1id,
            class1name, relname, class2id,
            class2name)

10        END FOR

11      END FOR

12      RETURN (outputlist)

END
```

3.4 Ontology Quality Assessment Module.

In this module, the proposed ontology is evaluated. This assessment process is applied twice, once following the development module and once following the enrichment module. The ontology's quality can be assessed in multiple ways. In this case study, to overcome the absence of gold standard ontology in the e-government domain, the OntoMetrics quantitative measures are applied. They were utilized in [14] and the evaluation results of 20 ontologies from the e-government area were documented. This makes it easier to assess and compare the outcome of the suggested architecture. The calculations of these metrics and their correlation to ontology assessment dimensions are displayed in Table 4 and Table 5, respectively.

Table 2: AML matcher results – lexicon and relationship map

Ontology	Classes	Labels	Properties	Direct is-a Relations	Disjoint Clauses
O_4	18	24	21	37	12
O_{11}	11	11	10	18	0
O_{12}	8	8	10	12	0
O_{13}	8	8	12	12	0
O_{14}	126	126	4	248	0
O_{15}	17	17	13	33	0
O_{16}	50	150	77	107	3
O_{17}	98	97	118	-	-
O_{18}	2509	13809	129	5637	0
O_{19}	209	458	198	327	0
EGYGOV	**125**	**122**	**95**	**200**	**39**

Table 3: AML matcher results – mappings

Ontology	No of Mappings
O_4	**0**
O_{11}	**8**
O_{12}	**1**
O_{13}	**1**
O_{14}	**4**
O_{15}	**4**
O_{16}	**33**
O_{17}	**21**
O_{18}	**122**
O_{19}	**42**

4 Experimental Results

This section presents the experimental results of the proposed case study. The dataset contains 20 of the existing ontologies in the domain of e-government. Their OntoMetrics measurements are outlined in [31]. Table 6

Table 4: OntoMetrics calculations [44]

Category	Metric	Equation	Description
Schema Metrics	Attribute Richness (AR)	$AR = \frac{\|att\|}{\|C\|}$ (1)	|att| is the total number of attributes |C| is the total number of classes in the ontology
Schema Metrics	Inheritance Richness (IR)	$IR = \frac{\|H\|}{\|C\|}$ (2)	|H| is the number of subclass relations |C| is the total number of classes
Schema Metrics	Relationship Richness (RR)	$RR = \frac{\|P\|}{\|H\|+\|P\|}$ (3)	|P| is the number of non-inheritance relations |H| is the number of inheritance relations
Knowledge Base Metrics	Average Population (AP)	$AP = \frac{\|I\|}{\|C\|}$ (4)	|I| is the total number of instances of the knowledge base |C| is the total number of classes
Knowledge Base Metrics	Class Richness (CR)	$CR = \frac{\|C\prime\|}{\|C\|}$ (5)	|C'| is the number of classes in the knowledge base |C| is the total number of classes
Graph Metrics	Absolute Root Cardinality (ARC)	$ARC = n_{ROO\subseteq g}$ (6)	$n_{ROO\subseteq g}$ represents the number of elements in the set of root nodes *ROO* in the directed graph *g*
Graph Metrics	Absolute Leaf Cardinality (AC)	$AC = n_{LEA\subseteq g}$ (7)	$n_{LEA\subseteq g}$ represents the number of elements in the set of leaf nodes *LEA* in the directed graph *g*
Graph Metrics	Average Depth (AD)	$AD = \frac{1}{n_{P\subseteq g}}\sum_{j}^{P} N_{j\in P}$ (8)	P represents the set of paths in the directed graph g $n_{P\subseteq g}$ is the number of elements in P $N_{j\in P}$ is the number of elements on the path j.
Graph Metrics	Maximum Depth (MD)	$MD = N_{j\in P}\forall i\exists j(N_{j\in P} \geq N_{i\in P})$ (9)	$N_{j\in P}$ is the number of elements on the path *j* $N_{i\in P}$ is the number of elements on the path *i* which belong to the set of paths *P* in the directed graph *g*
Graph Metrics	Average Breadth (AB)	$AB = \frac{1}{n_{L\subseteq g}}\sum_{j}^{L} N_{j\in L}$ (10)	*L* represents the set of levels in the directed graph g $n_{L\subseteq g}$ is the number of elements in L $N_{j\in L}$ is the number of elements on the level j.
Graph Metrics	Maximum Breadth (MB)	$MB = N_{j\in L}\forall i\exists j\left(N_{j\in L} \geq N_{i\in L}\right)$ (11)	$N_{j\in L}$ and $N_{i\in L}$ are the number of elements on the level j and i respectively that belong to the set of levels L in the directed graph g

Table 5: OntoMetrics and ontology dimensions correlation [44]

Dimension	Description	Metrics
Accuracy	Determines how well the ontology represents the real-world domain	Equations (1), (2), (3), (8), (9), (10), and (11)
Understandability	Indicates the comprehension of the elements of the ontology	Equation (7)
Cohesion	Assesses how closely classes are related to one another	Equations (6) and (7)
Conciseness	Affects the extent to which the ontological information is beneficial	Equations (4) and (5)

illustrates the comparison between them and the proposed ontology's metrics. And to have an overall view, Table 7 summarizes the average value for all metrics and each dimension separately, moreover, the percentile [28] at which the average lies. The following sections discuss these findings.

4.1 Overall Metrics

In the case of EGYGOV's development outcome, the

Table 6: OntoMetrics results of e-government ontologies

Ontology	AR	IR	RR	AP	CR	ARC	AC	AD	MD	AB	MB
O_1	0.59099	0.136364	0.930233	0.681818	0.090909	19	19	1.136364	2	5.5	19
O_2	0.315789	0.736842	0.222222	0.526316	0.105263	7	10	3.033333	5	2.142857	7
O_3	0	1	0.346154	0.352941	0.058824	2	10	3.285714	5	2.33333	4
O_4	0.076923	1.230769	0.407407	0	0	3	10	2.076923	3	3.25	6
O_5	0.067797	0.779661	0.577982	0.016949	0.016949	15	42	2.836066	6	3.388889	15
O_6	0.666667	1.333333	0.5	1.166667	0.333333	3	2	1.5	2	1.5	3
O_7	0.033708	1.601124	0.2711	0.134831	0.02809	26	112	3.419162	6	3.604317	33
O_8	0.666667	1.333333	0.5	1.166667	0.333333	3	2	1.5	2	1.5	3
O_9	7.416667	7.333333	0.169811	26	0.583333	1	8	3.416667	4	2.4	4
O_{10}	0.106061	1.515152	0.602386	1.386364	0.530303	26	92	2.447368	4	4.956522	26
O_{11}	0.363636	0.818182	0.25	4.727273	0.272727	2	7	2.727273	4	2.2	3
O_{12}	0.375	0.75	0.4	1.375	0.125	2	6	2.375	3	2.666667	5
O_{13}	0.75	0.75	0.333333	1.875	0.125	2	6	2.25	3	2.666667	4
O_{14}	0	0.984127	0	0.992063	0.007937	2	107	3.801587	4	6.3	17
O_{15}	0	1	0.346154	0.352941	0.058824	2	10	3.285714	5	2.333333	4
O_{16}	0.36	2.12	0.341615	0.54	0.12	22	22	1.3125	2	2.909091	22
O_{17}	0.217391	1.978261	0.172727	0.652174	0.434783	16	56	3.009709	6	2.575	16
O_{18}	0.042231	1.130279	0.003862	0	0						
O_{19}	0.133333	1.148148	0.093567	0	0	8	112	3.639706	5	5.666667	25
O_{20}	0.4375	0.75	0.813956	1.90625	0.5	8	26	1.84375	3	4.571429	9
EGYGOV (Development Outcome)	**0.436508**	**1.571429**	**0.171548**	**0.880952**	**0.055556**	**1**	**114**	**3.188976**	**4**	**9.769231**	**45**
EGYGOV (Enrichment Outcome)	**0.772947**	**1.074879**	**0.044039**	**0.992754**	**0.310386**	**46**	**605**	**3.347107**	**8**	**8.144231**	**46**

average of all OntoMetrics measurements equals 16.37. This makes the proposed ontology the second one among the 20 ontologies and locates it in the 90th percentile, while O_7 comes in the first percentile (95th). On the other hand, after applying the enrichment module, results of eight metrics are enhanced. Therefore, the average is raised to 65.43. EGYGOV becomes the highest one among the 20 ontologies with a 95th percentile, while O_7 becomes the second one (90th percentile). These results are illustrated in Figure .6.

4.2 Accuracy

The average of accuracy-related metrics is the highest for both outcomes of EGYGOV and falls on the 95th percentile. The enrichment module enhances the results of four metrics out of seven while IR, RR and AB return lower values in case of enrichment outcome than development outcome. This low IR means that classes and relations injected into EGYGOV increase the depth and detailed coverage of the e-government domain. While low RR is brought on by the matcher returning only is-a relationships. As a result, inheritance relations are increased in contrast to other types of relations. So, it is better to define more non-inheritance relations in EGYGOV. Finally, the low value of AB indicates that EGYGOV's final outcome focuses on the vertical modeling of hierarchies rather than the horizontal modeling.

4.3 Understandability

The leaf nodes (AC) of the EGYGOV are the highest (95th percentile) in both outcomes. This large metric resolves the ambiguity of the ontology classes and relations. As a result, it leads to good understandability that will help domain experts to easily understand the ontology.

4.4 Cohesion

The average of both graph metrics ARC and AC in case of development outcome lies in the 80th percentile. This iscaused because of low number of root nodes in that outcome. But the average is moved to the 95th percentile after applying the enrichment module. The higher values of

Table 7: OntoMetrics - average and percentile

Ontology	All Metrics		Metrics correlated to Accuracy		Metrics correlated to Understandability		Metrics correlated to Cohesion		Metrics correlated to Conciseness	
	AVG	Percentile	AVG	Percentile	AVG	Percentile	AVG	Percentile	AVG	Percentile
O_1	6.19	57%	4.18	62%	19	50%	19	55%	0.39	43%
O_2	3.28	43%	2.64	43%	10	30%	8.5	45%	0.32	33%
O_3	2.58	29%	2.28	29%	10	30%	6	30%	0.21	24%
O_4	2.64	38%	2.29	38%	10	30%	6.5	40%	0	0%
O_5	7.79	67%	4.09	52%	42	65%	28.5	65%	0.02	14%
O_6	1.55	5%	1.50	5%	2	0%	2.5	0%	0.75	62%
O_7	16.92	90% or 95%	6.85	90%	112	85%	69	95%	0.08	19%
O_8	1.55	5%	1.50	5%	2	0%	2.5	0%	0.75	62%
O_9	5.85	52%	4.11	57%	8	25%	4.5	20%	13.29	95%
O_{10}	14.50	81%	5.66	81%	92	75%	59	85%	0.96	76%
O_{11}	2.49	24%	1.91	14%	7	20%	4.5	20%	2.50	90%
O_{12}	2.19	19%	2.08	24%	6	10%	4	10%	0.75	62%
O_{13}	2.16	14%	1.96	19%	6	10%	4	10%	1.00	81%
O_{14}	12.92	76%	4.58	76%	107	80%	54.5	75%	0.50	52%
O_{15}	2.58	29%	2.28	29%	10	30%	6	30%	0.21	24%
O_{16}	6.88	62%	4.43	71%	22	55%	22	60%	0.33	38%
O_{17}	9.37	71%	4.28	67%	56	70%	36	70%	0.54	57%
O_{18}	0.24	0%	0.39	0%					0	0%
O_{19}	14.61	86%	5.81	86%	112	85%	60	90%	0	0%
O_{20}	5.17	48%	2.92	48%	26	60%	17	50%	1.20	86%
EGYGOV (Development Outcome)	**16.37**	**90%**	**9.16**	**95%**	**114**	**95%**	**57.5**	**80%**	**0.47**	**48%**
EGYGOV (Enrichment Outcome)	**65.43**	**95%**	**9.63**	**95%**	**605**	**95%**	**325.5**	**95%**	**0.65**	**57%**

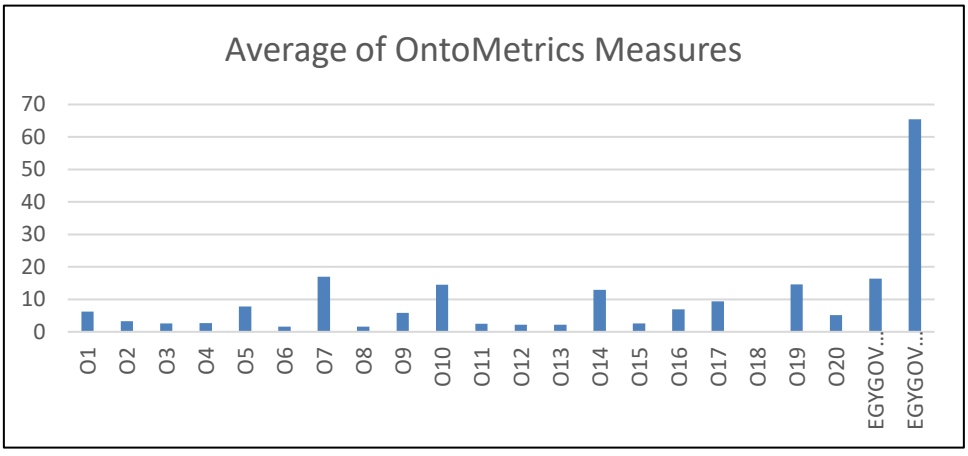


Figure 6: Average of onto metrics measures

both metrics in the EGYGOV's final outcome lead to the same conclusion, which is that the ontology accurately describes the e-government domain using a large number of inheritance relations. This also supports the idea that classes are well connected to each other.

4.5 Conciseness

This dimension is measured via the number of instances and their distribution among classes. The average of those metrics in the case of development and enrichment outcomes lies in percentiles 48% and 57%, respectively. Low AP and CR metrics are the reason why the average is relatively low. Low AP means that the instances defined into the knowledgebase is insufficient to populate all of the knowledge. While low CR indicates that the knowledgebase lacks data that fully demonstrates all of the available classes. This can be justified because EGYGOV has relatively high number of classes (125 classes in the development outcome and 828 classes in the enrichment outcome). So, to return high values in this dimension, a huge number of instances need to be defined and populated across all the classes. It is noticed that the same scenario applies to other ontologies that have a greater number of classes such as O_{14}, O_{18} and O_{19} (as displayed in Table 2). For two of them their average is located in the 0^{th} percentile, and the third one is located in 52^{nd} percentile.

5 Conclusion And Future Work

This research presents an enhanced ontology engineering architecture for building domain ontologies from scratch. This architecture is based on ODCM and ontology matching. With the help of this architecture, users can complete ontology development tasks since it provides guidance for all key activities, from requirement specification to ontology evaluation. It is composed of four main modules: Requirement Specification, Ontology Development, Ontology Enrichment, and Ontology Quality Assessment. The proposed architecture is applied to the domain of e-governance in Egypt. The results are encouraging when the produced ontology is compared to 20 existing ontologies from the same domain. On the basis of OntoMetrics, the average of metrics related to accuracy, understandability, cohesion and conciseness lies in 95^{th}, 95^{th}, 95^{th} and 57^{th} percentiles respectively. The results can be enhanced by increasing the non-inheritance relations and by distributing the instances across all classes. The three main contributions of this study are: (1) the combination of ODCM conceptual modeling with ontology matching, (2) two new algorithms for the selection of the most relevant ontology and the extraction of new classes and relations, as well as (3) the new domain ontology for the Egyptian e-government.

In the future, it is planned to 1) apply the proposed architecture to various domains. 2) enrich the ontology with new constraints to increase its expressiveness; and 3) employ other methods in the assessment process.

References

[1] R. Abaalkhail, *Ontology Based Framework for Conceptualizing Human Affective States and Their Influences*, Doctoral Dissertation, Université d'Ottawa/University of Ottawa, 2018.

[2] E. Abrahão and A. R. Hirakawa, "Complex Task Ontology Conceptual Modelling: Towards the Development of the Agriculture Operations Task Ontology," *KEOD*, 2:285-292, 2018.

[3] A. Q. Al-Namiy, "Algorithm to Match Ontologies on the Semantic Web," *Int J Adv Comput Sci Appl*, 4(3):221-227, 2013.

[4] S. Al-Yadumi, W. W. Goh, E. X. Tan, N. Z. Jhanjhi, and P. Boursier, "Multimatcher Model to Enhance Ontology Matching Using Background Knowledge," *Information,* Switzerland, 12(11):487, doi: 10.3390/info12110487, Nov. 2021.

[5] J. Antonio and T. Saorín Pérez, "A Conceptual Model for an OWL Ontology to Represent the Knowledge of Transmedia Storytelling," 15th International ISKO Conference, pp. 511-520, 2018.

[6] N. Alrebdi and N. Khan, "Core Elements Impacting Cloud Adoption in the Government of Saudi Arabia," *Int J Adv Comput Sci Appl*, 13(6):270-273, 2022.

[7] W. Boggs and M. Boggs, *Mastering UML with Rational Rose 2002,* Alameda: Sybex, Vol. 1, 2002.

[8] S. Debbech, S. Collart-Dutilleul, and P. Bon, "An Ontological Approach to Support Dysfunctional Analysis for Railway Systems Design," *Journal of Universal Computer Science*, 26(5):549-582, 2020.

[9] T. Derave, "A Reference Architecture for Customizable Marketplaces," International Conference on Conceptual Modeling, pp. 222–229. doi: 10.1007/978-3-030-34146-6_20, 2019.

[10] T. Derave, T. P. Sales, M. Verdonck, F. Gailly, and G. Poels, "Domain Ontology for Digital Marketplaces," International Conference on Conceptual Modeling, pp. 191-200, 2019.

[11] "Egyptian E-Government Portal." http://www.egypt.gov.eg/english/home.aspx (accessed Aug. 04, 2022).

[12] H. Elasri, A. Sekkaki, and L. Kzaz, "An Ontology-Based Method for Semantic Integration of Business Components," *2011 11th Annual International Conference on New Technologies of Distributed Systems, NOTERE 2011 – Proceedings*, pp. 1-8. doi: 10.1109/NOTERE.2011.5957993, 2011.

[13] D. Faria, C. Pesquita, E. Santos, M. Palmonari, I. F. Cruz, and F. M. Couto, "LNCS 8185 - The AgreementMakerLight Ontology Matching System," OTM Confederated International Conferences on the Move to Meaningful Internet Systems, Springer, Berlin, Heidelberg, pp. 527-541, September 2013.

[14] J. V. Fonou-Dombeu and S. Viriri, "OntoMetrics Evaluation of Quality of e-Government Ontologies," International Conference on Electronic Government

and the Information Systems Perspective, pp. 189-203, 2019.

[15] N. G'abor, "Ontology Development," Semantic Web Services, pp. 107-134, 2007.

[16] A. Gal, "Ontology Engineering," in *Encyclopedia of Database Systems*, New York, NY: Springer New York, pp. 2584-2585. doi: 10.1007/978-1-4614-8265-9_1315, 2018.

[17] A. García S, G. Guizzardi, O. Pastor, V. C. Storey, and A. Bernasconi, "An Ontological Characterization of a Conceptual Model of the Human Genome," *International Conference on Advanced Information Systems Engineering*, pp. 27–35. doi: 10.1007/978-3-031-07481-3_4, 2022.

[18] T. R. Gebba and M. R. Zakaria, "E-Government in Egypt: An Analysis of Practices and Challenges," *International Journal of Business Research and Development*, 4(2):11-25, 2015.

[19] J. Guerson, T. P. Sales, G. Guizzardi, and P. A. Almeida, "OntoUML Lightweight Editor A Model-Based Environment to Build, Evaluate and Implement Reference Ontologies," 2015 IEEE 19th International Enterprise Distributed Object Computing Workshop, pp. 144-147, 2015.

[20] G. Guizzardi, *Ontological Foundations for Structural Conceptual Models*, PhD Thesis, Centre for Telematics and Information Technology, University of Twente, 2005.

[21] G. Guizzardi, "Theoretical Foundations and Engineering Tools for Building Ontologies as Reference Conceptual Models," *Semant Web*, 1(1,2):3-10, 2010.

[22] G. Guizzardi, G. Wagner, J. Paulo, A. Almeida, and R. S. Guizzardi, "Towards Ontological Foundations for Conceptual Modeling: The Unified Foundational Ontology (UFO) Story," *Appl Ontol*, 10(3–4):259-271, 2015.

[23] M. Haggag, S. Fathy, and N. Elhaggar, "Ontology-Based Textual Emotion Detection," *Int J Adv Comput Sci Appl*, 6(9):239-246, 2015.

[24] J. Hartmann, R. Palma, and Y. Sure, "OMV-Ontology Metadata Vocabulary," *ISWC*, Vol. 3729, 2008.

[25] K. Hussein Shafa and J. Omer Atoum, "A Framework for Improving the Performance of Ontology Matching Techniques in Semantic Web," *Int J Adv Comput Sci Appl*, 3(1):8-14, 2012.

[26] T. Jonsson and H. Enquist, "Phenomenological Ontology Guided Conceptual Modeling for Enterprise Information Systems," International Conference on Conceptual Modeling, pp. 31-34, 2018.

[27] H. Lamharhar, D. Chiadmi, and L. Benhlima, "Moroccan e-Government Strategy and Semantic Technology," Government e-Strategic Planning and Management, pp. 323–343, 2014.

[28] E. Langford, "Quartiles in Elementary Statistics," *Journal of Statistics Education*, 14(3):1-27, doi: 10.1080/10691898.2006.11910589, Jan. 2006.

[29] X. Liu, Q. Tong, X. Liu, and Z. Qin, "Ontology Matching: State of the Art, Future Challenges, and Thinking Based on Utilized Information," *IEEE Access*, 9:91235-91243, doi: 10.1109/ACCESS.2021.3057081, 2021.

[30] M. A. Musen, "The Protégé Project: A Look Back and a Look Forward," *AI Matters*, 1(4):4-12, June 2015.

[31] J. C. Nardi, R. de Almeida Falbo, J. P. A. Almeida, G. Guizzaardi, L. F. Pires, M. J. van Sinderen, N. Guarino, and C. M. Fonseca, "A Commitment-Based Reference Ontology for Services," *Inf Syst*, 54:263-288, Dec. 2015.

[32] D. Oliveira and C. Pesquita, "Improving the Interoperability of Biomedical Ontologies with Compound Alignments," *J Biomed Semantics*, 9(1):1-13, doi: 10.1186/s13326-017-0171-8, Jan. 2018.

[33] D. Porello, G. Guizzardi, T. P. Sales, and G. Amaral, "A Core Ontology for Economic Exchanges," International Conference on Conceptual Modeling, pp. 364–374, 2020.

[34] M. Poveda-Villalón, A. Fernández-Izquierdo, M. Fernández-López, and R. García-Castro, "LOT: An Industrial Oriented Ontology Engineering Framework," *Eng Appl Artif Intell*, 111:104755, doi: 10.1016/j.engappai.2022.104755, May 2022.

[35] P. Sacco, R. Gallo, and F. Mazzetto, "Farm Ontology: A System Thinking Approach for Planning and Monitoring Farm Activities," *Proceedings of the 3rd LeNS World Distributed Conference*, pp. 429-434, 2019.

[36] C. Silva and O. Belo, "A Core Ontology for Brazilian Higher Education Institutions," *CSEDU*, pp. 377–383, 2018.

[37] M. C. Suárez-Figueroa, A. Gómez-Pérez, and M. Fernández-López, "The Neon Methodology for Ontology Engineering," *Ontology Engineering in a Networked World*, Springer Berlin Heidelberg, pp. 9-34, 2012.

[38] M. Suchánek, "OntoUML Specification Documentation," https://ontouml.readthedocs.io/en/latest/, 2020.

[39] R. Syed and H. Zhong, "Cybersecurity Vulnerability Management: An Ontology-Based Conceptual Model," 24th Americas Conference on Information Systems, *AMCIS*, pp. 16-18, 2018.

[40] J. Trujillo, K. C. Davis, X. Du, E. Damiani, and V. C. Storey, "Conceptual Modeling in the Era of Big Data and Artificial Intelligence: Research Topics and Introduction to the Special Issue," *Data and Knowledge Engineering*. Elsevier B.V., 135:101911, doi: 10.1016/j.datak.2021.101911 Sep. 01, 2021.

[41] United Nations, "UN E-Government Survey," https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/53-Egypt/dataYear/2020 (accessed Aug. 04, 2022).

[42] C. F. Uwasomba, Y. Lee, Z. Yusoff, and T. M. Chin,

"Ontology-Based Methodology for Knowledge Acquisition from Groupware," *Applied Sciences,* Switzerland, 12(3):1448, doi: 10.3390/app12031448, Feb. 2022.

[43] M. Verdonck and F. Gailly, "Insights on the Use and Application of Ontology and Conceptual Modeling Languages in Ontology-Driven Conceptual Modeling," *International Conference on Conceptual Modeling*, LNCS, 9974:83-97, 2016.

[44] A. N. H. Zaied, A. H. Ali, and H. A. El-Ghareeb, "E-government Adoption in Egypt: Analysis, Challenges, and Prospects," *International Journal of Engineering Trends and Technology*, 52(2):70-79, Oct. 2017.

[45] M. R. Zein and H. Twinomurinzi, "Towards Blockchain Technology to Support Digital Government," International Conference on Electronic Government and the Information Systems Perspective, pp. 207–220, 2019.

SHAIMAA HARIDY received the B.Sc. and M.Sc. degrees in information systems from the Faculty of Computer and Information Sciences (FCIS), Ain Shams University (ASU), Egypt, in 2004 and 2011, respectively. Her master's was about Representation of Ontologies for Semantic Web Services. She is currently an Assistant Lecturer with FCIS, ASU. Her research interests include artificial intelligence, semantic web, ontology engineering, and software engineering.

RASHA ISMAIL received the Ph.D. degree in data mining and data warehousing from Ain Shams University, Egypt, in 2009. She was the Director of the credit hours programs, from 2013 to 2019. She has contributed in implementing of the current credit-hour curriculum for the undergraduate programs of bioinformatics and software engineering at Ain Shams University, where she is currently a Professor and the Vice Dean of postgraduate studies and research affairs with the Faculty of Computer and Information Sciences. In addition, she is also the Director of the Ain Shams Portal. Her current research interests include data science, software engineering, information retrieval, big data analytics, data mining, and bioinformatics.

NAGWA BADR received the M.S. degree in computer science and the Ph.D. degree in software engineering and distributed systems from Liverpool John Moores University, U.K., in 1996 and 2003, respectively. She had done postdoctoral studies with Glasgow University, U.K. She is currently a Professor and the Dean of the Faculty of Computer and Information Sciences (FCIS), Ain Shams University (ASU). For the last few years, she is the Head of committee that contributed to research projects funded by national and international grants in information systems, bioinformatics, business analytics, and health informatics. Her research interests include software engineering, cloud computing, big data analytics, social networking, Arabic search engines, and bioinformatics.

MOHAMED HASHEM was the Head of the Information Systems Department, FCIS. He was the Vice Dean of education and student affairs at the Faculty of Computer and Information Sciences (FCIS). He is currently a Professor in information systems with FCIS, Ain Shams University, Egypt. His research interests include modeling and simulation of computer networks, computer security, and data management.

Index

Authors

A

B

C

D-G

H-J

K-L

M-O

W

P-Q

X-Z

R-S

T-V

Key Words

A

B-C

D

E-F

G-H

I-J

K-L

Journal Submission

The International Journal of Computers and Their Applications is published four times a year with the purpose of providing a forum for state-of-the-art developments and research in the theory and design of computers, as well as current innovative activities in the applications of computers. In contrast to other journals, this journal focuses on emerging computer technologies with emphasis on the applicability to real world problems. Current areas of particular interest include, but are not limited to: architecture, networks, intelligent systems, parallel and distributed computing, software and information engineering, and computer applications (e.g., engineering, medicine, business, education, etc.). All papers are subject to peer review before selection.

A. Procedure for Submission of a Technical Paper for Consideration

1. Email your manuscript to the Editor-in-Chief, Dr. Ajay Bandi. Email: ajay@nwmissouri.edu.
2. Illustrations should be high quality (originals unnecessary).
3. Enclose a separate page (or include in the email message) the preferred author and address for correspondence. Also, please include email, telephone, and fax information should further contact be needed.
4. **Note**: Papers shorter than 10 pages long will be returned.

B. Manuscript Style:

1. **WORD DOCUMENT**: The text should be **double-spaced** (12 point or larger), **single column** and **single-sided** on 8.5 X 11 inch pages. Or it can be single spaced double column.

   LaTex DOCUMENT: The text is to be a double column (10 point font) in pdf format.
2. An informative abstract of 100-250 words should be provided.
3. At least 5 keywords following the abstract describing the paper topics.
4. References (alphabetized by first author) should appear at the end of the paper, as follows: author(s), first initials followed by last name, title in quotation marks, periodical, volume, inclusive page numbers, month and year.
5. The figures are to be integrated in the text after referenced in the text.

C. Submission of Accepted Manuscripts

1. The final complete paper (with abstract, figures, tables, and keywords) satisfying Section B above in **MS Word format** should be submitted to the Editor-in-Chief. If one wished to use LaTex, please see the corresponding LaTex template.
2. The submission may be on a CD/DVD or as an email attachment(s). **The following electronic files should be included:**
   - Paper text (required).
   - Bios (required for each author).
   - Author Photos are to be integrated into the text.
   - Figures, Tables, and Illustrations. These should be integrated into the paper text file.
3. Reminder: The authors photos and short bios should be integrated into the text at the end of the paper. All figures, tables, and illustrations should be integrated into the text after being mentioned in the text.
4. The final paper should be submitted in (a) pdf AND (b) either Word or LaTex. For those authors using LaTex, please follow the guidelines and template.
5. Authors are asked to sign an ISCA copyright form (http://www.isca-hq.org/j-copyright.htm), indicating that they are transferring the copyright to ISCA or declaring the work to be government-sponsored work in the public domain. Also, letters of permission for inclusion of non-original materials are required.

Publication Charges

After a manuscript has been accepted for publication, the contact author will be invoiced a publication charge of **$500.00 USD** to cover part of the cost of publication. For ISCA members, publication charges are **$400.00 USD** publication charges are required.

Revised 2020