Analysis of Security Challenges in Cloud Computing Adoption for the Banking Sector

Kalim Qureshi*
College of Life Sciences, Kuwait University, Kuwait.
Sumaia Haider Sadeq†
College of Life Sciences, Kuwait University, Kuwait.
Paul Manuel ‡
College of Life Sciences, Kuwait University, Kuwait .

Abstract

Cybersecurity is a challenge in every field, but it poses a bigger challenge to finance institutions because the cost of recovering from a cybersecurity attack is enormous and time-consuming. Security becomes a bigger concern when finance institutions move into Cloud Computing (CC) technology because clouds are outsourced to third party vendors. That is why, the banking sectors still have concerns about CC adoption. The concerns are mainly related to the security of financial data and these concerns become more valid if the data have to be deployed on machines that do not exist in the physical proximity of the country where the rules and regulations apply. This study is an overall evaluation of the banking sector's privacy, security, and trust issues in cloud computing. The data collection and analysis consist of mainly three parts, quantitative, qualitative, and experimental evaluation. The quantitative part consists of a systematic literature review (SLR) of research articles from 2016 to 2020. A total of 623 publications were searched from six different databases, and 61 studies were filtered after applying inclusion and exclusion criteria. The second part consists of a qualitative study in which expert opinion is also collected in the form of interviews. Different issues are highlighted in SLR and by experts related to data privacy on cloud platforms. However, the ease of deployment, the optimal use of resources, and the reduction in maintenance costs are considered major advantages of cloud computing platforms. The third part of this study is identifying vulnerabilities and attack vectors in cloud computing platforms using a threat modelling framework. The STRIDE framework is used for threat modelling, and it reveals different vulnerabilities that exist in the cloud platform. For future work, an initial design of private cloud computing platforms is proposed for addressing data privacy, security, and regulatory compliance-related challenges for the banking sector.

ACM CCS (2012) Classification: Security and Privacy → Security Services

*College of Life Sciences, Kuwait University, Kuwait Email:kalimuddinqureshi@gmail.com.
†College of Life Sciences, Kuwait University, Kuwait. Email: sumaia.abul@gmail.com.
‡College of Life Sciences, Kuwait University, Kuwait Email: hfah66@yahoo.com.

Key Words:Cloud Computing, Cyber Security, cloud adoption in Banking, Systematic Literature Review.

1 Introduction

Financial sectors, primarily banks, are declared as critical infrastructure by the European Union. Basel Committee on Banking Supervision (BCBS) which is in Basel, Switzerland is a well-known European body working with international banks. Basel IV is a set of banking reforms based on international banking accords Basel I, Basel II and Basel III [1]. It was developed by BCBS and came into effect from 1 January 2023. BASEL provides a foundation of cybersecurity policies for the banking sectors. Basel IV lays guidelines for data trust and transparency while implementing cloud technology and subsequent cybersecurity protocols. The EU is recommending the banks of its member states to shift to a risk-centric approach "EU Cybersecurity Regulatory Framework" while migrating the data to clouds [2]. For the last few decades, the fastest growth in the field of Cloud Computing (CC) has been observed because of its wide range of deliverables for resources like computational storage, computational platforms, applications, and power to users through the Internet In today's market, the topmost cloud service providers are IBM, Amazon, Google, and Microsoft. The increasing demand for cloud computing from small companies to large-scale organizations increased the demand of protecting user information as well [3]. Major issues that are being tackled by cloud computing platforms are protecting, security, providing safety, and processing of the data that is being possessed by the user [4]. Different studies were conducted for software architecture in cloud computing [5]. However, there is a lack of studies about information security concerns related to cloud platform adoption in the banking sector. This research work aims to refresh and update the work conducted in the domain and provide more recent results and findings. It will identify and classify different topics, issues, and problems related to cloud computing [6]. Accordingly, the research is organized to provide a detailed review of different aspects of information security for cloud-based systems in banking. The research question is as follows:

"What are the issues, challenges, and solutions related to privacy, security, trust, and confidentiality in the adoption

of cloud-based systems for the banking sector?". The main contribution in this research work is following:

The main contributions of this research work are as follows:

1. An elaborate literature collection on privacy, security, and trust-related issues in the adoption of cloud computing for the banking sector.
2. An analysis of different types of vulnerabilities and attacks that exist in the cloud computing platform.
3. An analysis of mitigation protocols, models, and frameworks for malicious attacks on cloud computing platforms.
4. STRIDE threat model for a cloud computing platform that provides insight into the security analysis, thereby helping administrators to overcome security challenges.
5. A recommendation to Kuwait banks that are migrating to cloud systems.

This paper is not only a review paper, but it also investigates the following major components:

1. Systematic literature review.
2. Quantitative and qualitative analysis.
3. STRIDE threat modelling.
4. Interview analysis.
5. Proposed model.

The paper first discusses different related works. The next section explains the method adopted for conducting a systematic literature review, followed by the analysis of extracted studies. A threat modelling framework is applied to the results for the validation of the findings of the systematic literature review, and different countermeasures are proposed.

2 Related Works

The banking industry works for the economy of the nation therefore, they are a matter of national status and a source of revenue for people. Banking systems require security implementation in the form of digital certificates for devices such as One-Time Passwords (OTPs), protection and transaction monitoring and policies, and fraudulent and anti-money laundering detection systems [7]. Keeping the regulatory requirements up to date to protect the customer's data, cloud-based system devices play a vital role in terms of security measures for banking systems [8]. Banking and other sectors have a cyber-security department that deploys common safety measures to secure the systems. These security measures are Secure Socket Layers (SSL), Vulnerability and assessment testing of systems, Data encryption, Firewalls, Intrusion Detection Systems (IDS), Network Intrusion Prevention Systems (NIPS), Domain Name Systems (DNS), Password protection mechanisms and SMS alerts to clients [9-10]. All these security systems are used to secure cloud infrastructure in banking systems. However, there are still some risks and vulnerabilities due to exterior agents or unintentional errors occurring by the staff itself; therefore, data privacy and systems safety remains a significant concern. A statement of financial losses due to different cyber-attacks on banking systems is provided in Table 1 and a statement of losses in different domains is given in Table 2. This study provides a detailed systematic literature review of privacy, security and trust related issues in the banking sector for adopting cloud computing.

Table 1: Losses due to Cyber Attacks

	Data Breaches	Business Disruptions	Fraud	Other	Total
Frequency	53,500	4,915	56,308	692	115,415
Total Losses (USD million)	19,155.30	8,657	11,679.12	32.04	39,523.82

Table 2: Example of Financial Crime, Fraud, and Cybersecurity Costs ($million$)

Domain	Sub-domain	Loss	Total Loss
Regulatory fines and remediation	Reimbursement if any	50	150
	Regulatory fines	100	
Indirect costs and foregone revenue	System unavailable	40	200
	Failed authentication	40	
	Transaction decline	40	
	Customer experience impact/attrition	40	
	Incorrect risk categorization	40	
Direct fraud losses	Breaches	16.6	50
	Fraud losses	16.6	
	Cost of FIU	16.6	
Direct and indirect personal costs	Cyber breach	41.6	125
	Fraud	41.6	
	Financial crime	41.6	

3 Research Methodology

3.1 Planning Phase

Planning is the first step in answering the research question considered in the SLR study. The review addresses a specific group of audiences and is conducted in each context. PICOC (population, intervention, comparison, outcome, context) criteria is adopted as a foundation of the research question (Table 3). The research is organized to provide a detailed review of different aspects of information security for cloud-based systems in banking and what models, frameworks, and solutions are proposed by researchers to address these challenges. Literature is explored related to the topic of information systems on cloud-based platforms in the banking sector to achieve the objectives. Instead of selecting generic Google Scholar for searching the data [11], we selected high impact factor journals such as IEEE, ACM, Springer, and ScienceDirect [12]. The reason for selection is to maintain the quality of search results. The search terms are "cloud computing", "cloud", "information systems", "banking" and "bank". Connecting these search terms using Boolean operators results in these search phrases. Phrase: (bank OR banking) AND (information system) AND (cloud OR cloud computing). Figure 2 represents the data extraction steps from various databases. Figure 1 represents the research methodology steps for our SLR formation.

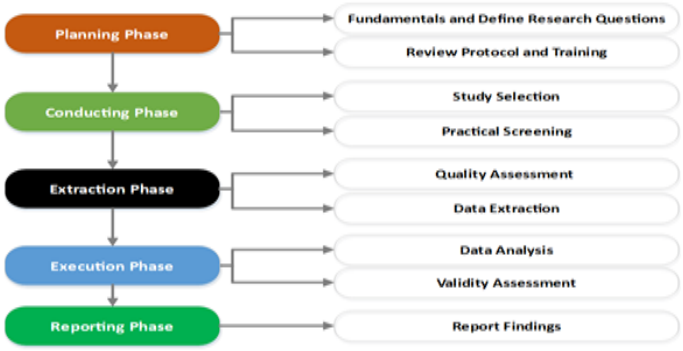

Figure 1: Research methodology in steps

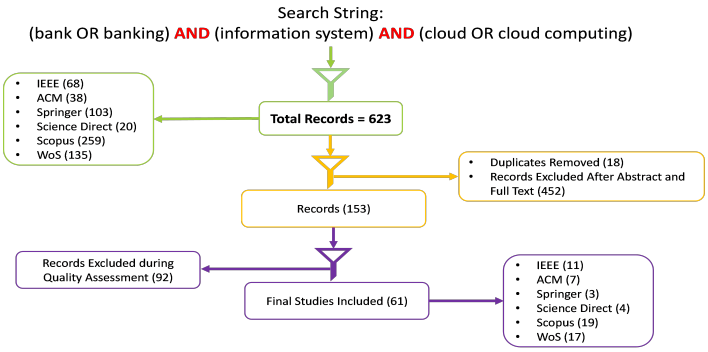

Figure 2: Data extraction from various databases

3.2 Conducting Phase

The conducting phase consists of the selection of studies and their screening based on inclusion and exclusion criteria and includes (1) The publication is between January 2016 to December 2020, (2) Apply the search on title, abstracts and keywords only, (3) Include articles published in the English language and (4) Search for journal publications only. The search string resulted in a total of 623 articles (Table 3). A large number of publications are retrieved from literature from six different databases. To get the answer to the research question, a filtering process is required. The irrelevant publications are excluded based on the following criteria:

• The selected study should answer the research question

• The selected study must explicitly address the inclusion and exclusion guidelines.

The reviewer decides to include the publication for the next step of quality assessment. The study is selected based on a brief review of the title and abstract. The inclusion and exclusion criteria given in Table 4 are a general guideline. The researcher has to consider valid justification and a reasonable number of publications that assist in answering the research questions. The result of the search query from each database and collected in the form of an excel sheet containing metadata information of publication such as title, abstract, date of publication, keywords, authors, and number of citations. The author shared this excel sheet with the co-researcher to either include or exclude the study by labelling yes or no in front of each publication. The selection of studies is based on inter-annotator agreement. According to the guidelines of training the reviewers provided [13], the reviewers are trained by 10 studies selected from the Science Direct database and their inter-rater reliability is calculated by finding the level of agreement among them. The disagreed studies are discussed, and the understanding of the second reviewer is improved for further interpretation. Overall, the inter-annotator agreements were 95%.

Source	URL	Articles Collected
IEEE	https://ieeexplore.ieee.org/search/advanced	68
ACM	https://dl.acm.org/search/advanced	137
Science Direct	https://www.sciencedirect.com/search	20
Springer	https://link.springer.com/advanced-search	103
Scopus	https://www.scopus.com/home.uri	259
Web of Science	https://mjl.clarivate.com/search-results	135
Total		**623**

Table 3: Selected Digital Libraries and Journals

Comparison	Okoli (Okoli & Schabram, 2010)	Kitchenham (Kitchenham, 2004)
Citation count	1606	6201
Target domain	Information systems	Software engineering
Guidelines	Six	Three
Phases	Four	Three
Data collection approach	Qualitative/quantitative	Only qualitative

Table 4: SLR Guidelines Comparison

3.3 Quality Assessment

The process of quality assessment eliminates the studies that do not help in answering the research question and are not part of the inclusion criteria. This section evaluates the selected studies based on inclusion and exclusion criteria and the knowledge that can be extracted from these studies for future research. The process of quality assessment is based on an in-depth review of selected studies to improve the quality standards of SLR. The initially collected studies based on inclusion/exclusion criteria do not fulfill quality criteria and thus, all of these studies cannot be made part of the final assessment in SLR [14]. The quality assessment process is based on a set of questions to assess the quality of selected studies. The criteria are called DARE criteria [15]. Table 5 provides a list of questions that are asked during the quality assessment of a study. The answer is “Yes” if the question meets the assessment criteria and “No” if it does not fulfill. If a study partially answers the research question, then a score of 0.5 can be given. After answering all the questions, the sum of all question scores is obtained. Based on a predefined threshold, if the sum is greater than the threshold, the study is included else excluded [16]. After quality assessment, only 61 studies are finally selected, and the process of selection is given in Figure 1.

Q ID	Question	Score
QA1	Is the objective of the article clearly defined?	Y/N
QA2	Does the article answer research questions?	Y/N/P
QA3	Is the research method described?	Y/N/P
QA4	Are the suggested countermeasures/solutions validated?	Y/N/P
QA5	Are the contributions and limitations of the article explained?	Y/N/P
QA6	Does the article provide a space for future work?	Y/N

Table 5: Quality Assessment Questions

Source	Total	Selected	Included	Excluded
IEEE	68	37	11	26
ACM	38	18	7	11
Science Direct	20	6	4	2
Springer	103	19	3	16
Scopus	259	63	19	38
Web of Science	135	28	17	11
Total	623	171	63	104

Table 6: Database Statistics

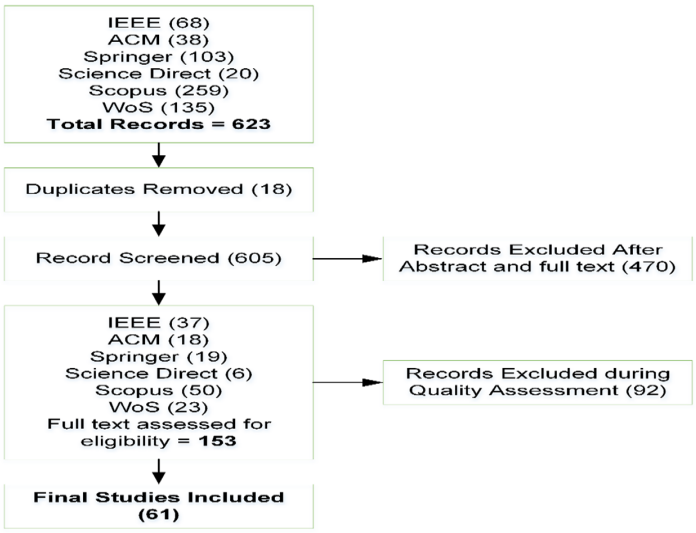

Figure 3: Filtration Process

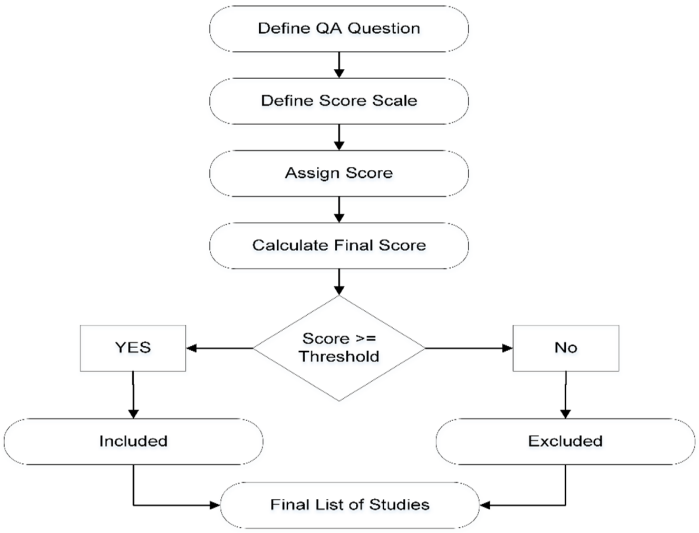

Figure 4: Quality Assessment Criteria.

4 Data Analysis

All the 61 studies are reviewed that are extracted after quality assessment. The data extraction considers the study reference, title, year of publication, privacy, security and trust issues, analysis method, and future works. The first three properties are related to the metadata information of the selected study. The rest of the properties assist in answering the research questions. The studies are extracted and evaluated for suitability with second researchers on the pilot set of studies to ensure any technical issues in the completeness [15]. The review of 138 selected papers is initiated by reading the complete paper. The review further helped to remove duplicate papers, irrelevant papers discussing cloud computing as an example, survey papers, and papers not related to security and privacy issues for the adoption of cloud platforms in the banking sector. Finally, 61 papers are selected for discussion in different extracted categories.

4.1 Application Security

Application security is concerned with the security of data shared through applications on cloud platforms. These applications could be mobile applications, web applications, or desktop applications. A cloud-based data sharing application is proposed [17]. This application consists of five phases which are system initialization by the group manager, mobile user registration phase, file upload by the mobile user, file download by a mobile user, and the mobile user revocation phase. The proposed protocol is found promising against Man-In-The-Middle (MITM) attacks, message modification attacks, and masquerading attacks. It ensures that even the group manager and the cloud cannot access the documents stored in the cloud.

A web service model is developed to choose the best available cloud centers considering the quality of service parameters such as response time, availability, security, and minimizing the cost of service [18]. The model is tested with 2507 data records using the TreeNet method and claimed to achieve 99% accuracy for optimal resource selection. An FPGA-based system for the security of cloud platforms is proposed [19]. This is an ARM-based FPGA solution that is efficient against six different attacks. This solution can be extended to heterogeneous cloud platforms. A four admin-based key exchange mechanism for secure banking transactions is proposed [20]. Every admin is provided with user-id, password, challenge-key and its corresponding challenge-response key, Attribute Based Encryption (ABE) key, and MAC and IP Address captured in Cloud. The servers generate a key which is distributed among admins with their privileges. A proxy re-encryption mechanism is proposed [21]. This application also ensures data security

through Advanced Encryption Standard (AES) by adopting a new subkey for each block of data. Information-Flow control mechanism between cloud platforms and users is proposed to ensure the integrity and confidentiality of information [22]. The system ensures the security of data through a hardware-based solution. The system is dynamic labelling based on information flow among decentralized systems. Cloud migration is one of the key requirements for the selection of cloud vendors during banking operations [23]. The research work provided in [24] claims the ineffectiveness of signature-based techniques such as NetFlow or traffic flow detection and Anomaly-based detection. It proposed a real-time bot detection system with high accuracy using a domain generation algorithm.

4.2 Authentication and Authorization

The multi-path authentication scheme is proposed for authenticated data transmission to increase security levels [25]. This multi-modal and multi-path data transmission to cloud machines makes it difficult for an adversary to intercept complete information. Considering the limitations of credit and debit card pins, a QR code-based user authentication mechanism is proposed [26]. A different authentication scheme using Sparse Matrix in cloud computing is proposed [27]. This approach used a trust matrix using swarm intelligence in cloud computing. Trust matrix is generated using the input by the user which is verified by the ant formed on three-levels, i.e. user, Cloud Data Storage (CDS), Cloud Service Provider (CSP). At each level, ants keep checking on the trust matrix. A new memory protection scheme based on a page-based authentication algorithm using Aggregate Message Authentication Code (AMAC) is proposed [28]. This scheme uses AMAC to compress the MAC of multiple memory blocks, reducing the meta-data overhead and saving a significant amount of memory space. A triple-stage verification process to establish the identity of bank clients is proposed [29]. Due to multiple factors, it is difficult to gain illegitimate access to the banking system from remote locations. The concept of using an offline authentication device, Off-PAD (Offline Personal Authentication Device) as a trusted device to support different forms of authentication is proposed [30]. The solution of using an image steganography application to hide important data or documents under an image before uploading them to cloud storage will help to avoid hackers' attacks. An application developed based on the Least Significant Bit (LSB) algorithm to encode information in the best quality image is proposed [31]. Another hardware authentication emulation-based solution is proposed [32]. The option of an extra token key after a one-time password to authenticate for data access on cloud storage is proposed [33]. The token is time-limited and geo-limited and controlled by a financial administrator. Biometric authentication refers to automated methods used to identify a person by the features such as the face, iris, vein, fingerprint, palm print, etc. A method to authenticate a user through orientation of finger veins or iris image input is proposed [34]. A two-factor-based authentication in digital banking using cloud services is proposed [35]. The first factor is voice assistant (for primary authentication) and beacon (for secondary authentication). A two-factor-based authentication scheme is proposed [36] based password and a QR code for authentication.

4.3 User Behaviour

A study was conducted to determine customer behaviour in using cloud platforms concerning trust, cost, security, and privacy [37]. A model based on TAM-DTM theory is proposed and data is collected from 162 bank customers. The results show that the security and privacy constructs exhibited a strong positive influence on perceived ease of use, perceived usefulness, and trust. The study concludes that perceived usefulness, perceived ease of use, cost, attitudes toward cloud, and trust significantly influence users' behavioural intention to adopt cloud computing. A visual notations-based framework on existing misuse case scenarios that can support the elicitation of various cloud dependability requirements [38]. The result of the pilot experiment shows that the extended misuse case-driven technique is credible and viable for the elicitation of cloud dependability requirements. A survey is conducted regarding the adoption of cloud computing in the banking sector and the opinion of users in building trust in the service provider and the possible relationship between observance of ethical practices and trust-building [39]. The survey reveals a positive correlation and regression between trust and ethics.

4.4 Data Science

Machine learning is being widely utilized in technology in different domains including banking. A data privacy-preservation model for cloud storage is proposed in [40]. The classification models work over the data encrypted with different public keys which are outsourced from multiple data providers. A botnet is a Trojan Horse malware attack that poses a serious threat to the banking and financial sector [41]. The study provides the classification of different types of botnet attacks on banking data on cloud platforms (Amazon Web Services) using different classifier methods. Security issues in Cloud Service Models (CSM) and cloud deployment models for banking organizations are discussed in [42]. According to a qualitative (interviews) study from 40 persons about the issues and risks of the adoption of cloud in the banking sector. The study identified the highest risk of "Trusted cloud" in 3rd party (providers) and program (software) security.

4.5 General Threats

Data security on communication channels is a big security threat. Providing end-to-end anonymous communication and data sharing involves different stakeholders such as network managers and cloud services providers that can temper the communication. A model against adversary attack is proposed by [43] that is suitable for delay-tolerant applications as

well. One of the major threats to data security in banking organizations is the insider threat. This threat could be due to third-party systems or poor authentication processes. Different types of insider threats are discussed in the study [44]. Open source private cloud platforms are a general preference of financial organizations. The study develops an open-source static analysis tool to determine the security vulnerabilities of such cloud platforms [45]. Maintaining the customer's privacy of banking data on cloud platforms is one of the more desirable features. The study [46] highlights the ways digitization is breaching customer privacy, changes required over digital platforms, and data collection frequency to preserve customers (an individual's) right of being left alone. Instead of technological issues as cyber threats, the study [47] emphasizes that the differences in the organizational culture of traditional banks and fintech, different strategic vision of top management, lack of qualified personnel, which makes it difficult for banks to transform for cooperation. The inclusion of verification procedures, integration of offline and online modes, the use of implicit factors, and consumer biometric behaviour.

4.6 Cryptography

Cryptography is one of the major techniques for data security applied to applications hosted on cloud platforms. The study [48] performs the cryptanalysis of mobile wallet and cloud server-based secure payment models. A cloud server is used to overcome computational overhead. The cryptanalysis of this scheme shows that this scheme is vulnerable to various security attacks like known session-specific temporary information attacks, cloud server bypassing attacks, untrusted cloud servers, and client colluding attacks and impersonation attacks and not enough secure. The research by [49] proposes a modification to the RSA algorithm to improve the execution time using the parallel processing power of modern-day multi-core architecture-based machines. A banking data encryption solution based on Password-Based Key Derivation Function (PBKDF2), Argon2, AES-256, and IDA algorithm is proposed [50]. Similarly, a dual encryption scheme based on Elliptic Curve Cryptosystem (ECC) and Advanced Encryption Standard (AES) for securing sensitive data is given in [51]. The objective of combining both of these encryption schemes is to minimize the delay factor and increase the robustness and security of data. Location is used as an encryption attribute along with symmetric cryptography and ciphertext policy – Attribute-based encryption (CP-ABE) to implement secure access control to the outsourced data [52]. The data integrity is ensured using the Message Authentication Code (MAC). Another approach to encrypting large-scale banking data is based on the Paillier algorithm [53]. The approach mainly uses the multiplicative property of homomorphic encryption to calculate total interest on an encrypted banking dataset. An improved authentication protocol based on the previous framework for data security in banking environments on cloud platforms is proposed [54]. A technique of data security on a cloud platform based on a game-theoretical approach is proposed [55]. This approach uses XTR (effective and compact subgroup trace representation) which has the property of semantic security. A group of players in the game-theoretic field such as networks, servers, operating systems, and storage devices is considered to construct interaction among each other. This interaction is useful in the field of financial economics. It is believed that game theory and its optimization is going to provide a suitable framework for the design of a crypto-cloud computing system that will be perceived as a strong technique and satisfy the needs of many participants and users of the cloud.

4.7 Regulatory and Compliance

Cloud-based Fintech companies are disrupting traditional banking models, signalling that highly regulated firms must adopt Cloud technologies [56]. This paper provides risks associated with the adoption of cloud technology in the banking sector and penalties for non-regulatory compliance. A study regarding cloud services, outsourcing, and the contractual issue are divided into three parts. The first part is about cloud services [57] that deal with key drivers such as time to market, real and perceived barriers, and cultural and technical aspects. The second part of the study deals with the regulation of cloud as 'outsourcing' [58]. It sets out how EU banking regulators have approached banks' use of cloud services and considers regulators' lack of cloud computing knowledge. The third part of the study key contractual issues that arise in negotiations between banks and cloud service providers, including data protection requirements, complexities caused by the layering of cloud services, termination, service changes, and liability [59].

4.8 Information Security Models and Frameworks

An adversary model to examine the security of lightweight browsers is proposed [60]. This model revealed vulnerabilities in four different browsers that allow attackers to obtain unauthorized access to the user's private data. Some browsers also reveal browser history, email contents, and bank account details. This research deals with the performance analysis of recent cloud data security models [61]. This paper proposes cloud data security models based on Business Process Modelling Notations (BPMN) and simulation results can reveal performance issues related to data security as part of any organization's initiative on Business process management (BPM). Banking datasets are very skewed and contain only a few samples of fraudulent transactions [62]. Due to data security and privacy, different banks are usually not allowed to share their transaction datasets. This problem makes it difficult to detect fraud. A novel framework is proposed in this model in which banks keep their data and the model computes distributed data and learns patterns from this federated dataset using triplet-like metric learning and designs a novel meta-learning-based classifier. To reduce the computational complexity of transaction data at edge devices and remove the bottleneck of payment authority, a Bitcoin-based payment mechanism

is proposed [63]. The users can transact directly without needing a bank. The banking community has apprehensions about adopting cloud computing platforms. A five-stage cloud computing framework for banking organizations. These stages are Cloud mobility and cloud banking applications, cloud service models, cloud deployment models, cloud risk management models, and cloud security models [64]. This framework claims to reduce security issues. Three different models based on encryption for data privacy and security on cloud platforms are proposed in [65]. This work also provides a comparison of different other techniques for privacy preservation. A model of smart card security based on Elliptical Curve Cryptography is proposed [66]. This model enables the users to use only one card for any applications and transactions anywhere, anytime with one unique ID. A technique for the detection of highly coordinated polymorphic botnet attacks on cloud platforms is proposed [24]. Virtual machines are hosted on cloud platforms and share the same kernel. There exists a risk that the VM can gain root access to the host machine and may manipulate the other VMs hosted on the same host operating system. This becomes a huge concern in the case of the banking sector when multi-tenant clients are processing their sensitive data on these VMs [67]. The paper discusses different techniques to maintain isolation among the VMs hosted on the same physical machine. A knowledge-based data security model is proposed to ensure the security of banking data [68]. Separate ontologies for the subject, object, and action elements are created and an authorization rule is framed by considering the inter linkage between those elements to ensure data security with restricted access. The security model is applied to the Software as a Service (SaaS) cloud model. A risk management model for banking cloud solutions is proposed in [64]. The model has five stages for a successful cloud computing framework in a banking organization. A secure data sharing mechanism for cloud users in groups through mobile platforms is proposed [17]. The authors claim that the share of group key processes can suffer from Man in the Middle attack. The security of cloud data is achieved through a deployment model that uses a one-time token that is time-limited and geo-limited as well [33]. This token is used by the customers to access data hosted on a cloud platform. The token is controlled and managed by an administrator. A framework for mobile commerce is proposed [69]. This framework uses wireless public key infrastructure (WPKI), Universal Integrated Circuit Card (UICC), and community cloud to achieve end-to-end security during data transfer. A single smart card-based user authentication scheme to prevent unauthorized access to the cloud is presented [70]. A single smart card serves as a single interface to access multifaceted electronic services like banking, healthcare, and employment. A business process optimization (BPO) model for the security of cloud computing platforms is proposed [71]. This model has efficiently provided security protection for up to twenty BPO companies with each having more than 1000 employees. Attribute-based encryption increases the data size and requires more storage space in the cloud to store the data. A technique based on Likert Scale assignment and Dichotomous Response Matrix generation reduces the sensitive and non-sensitive data classification complexity [72]. Cloud platforms for banking comply with international standards such as Payment Card Industry Data Security Standard (PCI DSS), International Organization for Standardization (ISO 9001:2015, ISO/IEC 27001:2013, ISO/IEC 27017:2015), and many other national security standards [73]. This paper proposed an analytical model built on the EC2 memory-optimized instance model.

5 Quantitative Analysis

The number of studies included or excluded from each of the databases is shown in Table 6. Scopus database showed maximum excluded studies whereas Science Direct has minimum excluded studies. The largest contribution of studies is from Scopus (19) and the smallest from Springer (3). IEEE showed maximum relevant studies related to Privacy, security, and trust-related issues in cloud computing for the banking sector. Figure 3 .shows the year-wise distribution of studies from the Year 2016 to 2020 (5 years) proving the growing interest and concerns of the banking community in the adoption of cloud computing for the banking sector. When comparing with studies, it is identified that data leakage and data theft are the most discussed issues in the studies while compliance and regulatory requirements are not discussed at strength. Most of the studies discussed encryption as a solution for maintaining privacy. The distribution of studies in different domains is shown in Table 7.

Issue	Frequency in papers
Data Security	29
Data Leak	6
Communication Security	6
User Authentication	11
Regulatory Compliance	4
Risk Management	3
Botnet Attacks	2

Table 7: Issues Discussed in Different Studies

Qualitative Assessment

We interviewed 50 domain experts and asked following questions:

Q1: What are the advantages of using Cloud Computing in the Banking sector?

Q2: What are the possible challenges of adopting cloud technologies for the banking sector?

Q3: Are there any security techniques for managing the security challenges of cloud computing?

Q4: What are general threats expected from adopting cloud computing in the banking sector related to users, data, networks

or applications?

Q5: How do we handle the security risks in the Cloud Computing platform?

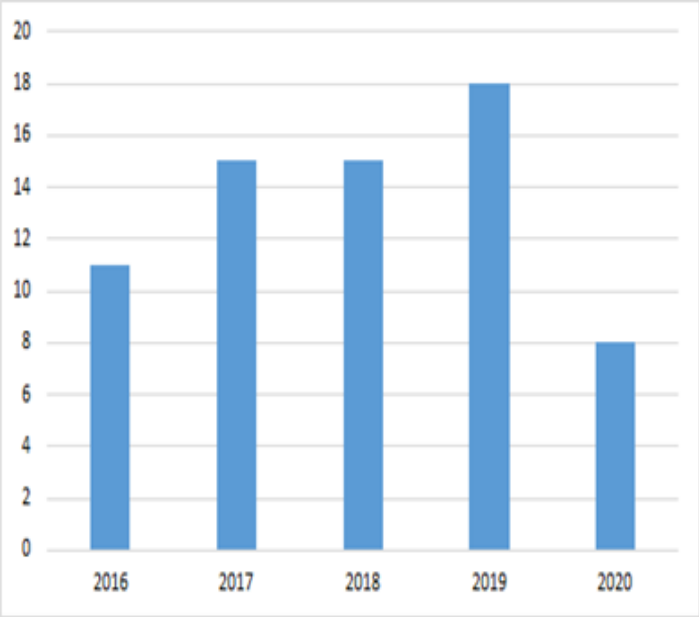

Figure 5: Year-wise Frequency of Studies

5.1 STRIDE Threat Model

STRIDE (Spoofing, Tampering, Repudiation, Denial of Service and Elevation of Privilege) is a famous threat model for identifying threats in a system or software [74]. It uses data flow diagrams to show the interaction among different components of the system or software. This process makes it easy to understand the threats at different levels of components. Generally, STRIDE covers flow of information at network layers and categorizes threats to particular categories along with a threat severity score [74].

In this study, the threat model provides an overview to the decision makers about potential threats in cloud computing environments related to privacy, security and trust related issues. Different threat categories, the violated property and its definition is provided in Table 8. The components of the threat modelling framework include a design of cloud computing platform, threat list, countermeasures list and preventive measures to overcome these challenges. All of these steps must be followed for the complete life cycle of STRIDE framework [75]. These steps are (1) Identify the assets of the system, (2) Identification of threats, (3) Rating of the threats and (4) Propose countermeasures.

A generic cloud computing model proposing the mitigation and overcoming of threats identified and categorized in Figure 4. This model is based on guidelines of STRIDE modelling and shows different components of the cloud computing model with the information flow among them.

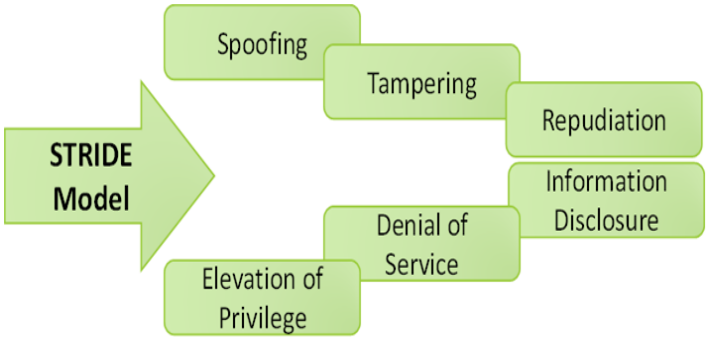

Figure 6: STRIDE Thread Modelling in steps

5.2 Identify Assets of the System

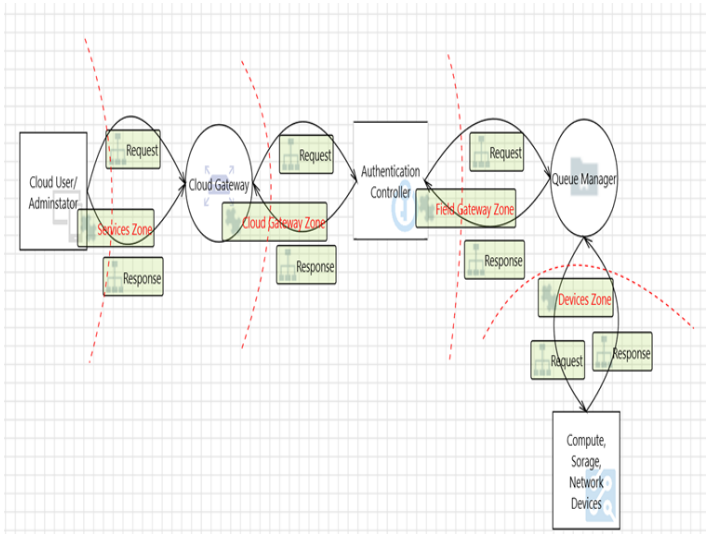

Figure 7: Cloud Threat Model

Several vendors provide cloud computing platforms for hosting banking applications and services. However, there is a basic set of components that is common among all platforms. These common components are storage devices, computing devices, networking equipment, security components, and cloud-management software (Figure 4). According to best practices of cloud infrastructure, the STRIDE threat model divides the cloud infrastructure into different zones [76]. These zones help in the identification of threat relevance to a particular boundary.

5.3 Identify Threats

In section 5.2, different threats are extracted related to cloud computing. For simplicity, the threats are generalized to understand the risk encountered by cloud users. These threats are generalized in Table given below according to the STRIDE category and the property violated. This conversion facilitates understanding of the risk from the non-security expert

background. Similar threats are combined in one category. For example, the communication on the network is intercepted through man-in-the-middle and spoofing attacks that fall under the category of active eavesdropping. It is important to note that most of the attacks on the cloud platform fall under the category of spoofing and information disclosure. Data leakage and data theft are categorized as one the major concerns and threats by the research community.

Table 8. Threats STRIDE Conversion [77]

STRIDE Categories	Extracted Threats	Countermeasure
Spoofing	Spoofing, impersonation, brute force attack, MITM, masquerade attack, unauthorized access	Authentication and Authorization Solutions (Identity Service)
Tampering	Forgery, malicious code injection, physical attack, unsecured interfaces, gain initial access	Port Blocking, Firewalls, and Single Point of Entry in the Cloud (Identity Service)
Information Disclosure	Data leakage, eavesdropping, insecure communication, abuse attack, open ports, replay attack	Storage of data in encrypted form. Only authorized users can access it. Ensured through Storage and Identity service
Denial of Service	DoS, DDoS, jamming, or interruption attacks	Detection and identification solutions
Elevation of Privilege	Over privileged, lack of authentication	Authentication and authorization solution (Identity service)

5.4 Rating the Threats

Rating the threats is the next process after the identification of threats. This process is necessary to prioritize the mitigation strategy. In some cases, few low priority threats can be ignored. The assessment is conducted using Microsoft DREAD (Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability) Framework. The answer to each question according to the DREAD risk factor is in the range of 1-3 [77]. Then after scoring all the risk factors calculate a total of each threat, if scores 5-7 the risk is low, 8-11 risk is medium, and 12-15 risk is high. Table 8 shows the threats rating for the extracted threats.

Vulnerability	D	R	E	A	D	Total	Priority
DDos or DOS	1	1	1	2	1	6	Low
Data leakage	3	3	3	3	2	13	High
Eavesdropping	3	2	3	2	3	13	High
Forgery	2	1	2	2	2	9	Medium
MITM	3	3	2	3	2	13	High
Lack of authentication	2	3	3	3	2	13	High
Unauthorized access	3	3	2	2	2	12	High
Malicious code injection	1	1	1	1	1	5	Low
Over privileged	3	1	1	2	2	9	Medium
Replay attack	1	1	1	1	1	5	Low
Physical attack	1	1	1	1	1	5	Low
Impersonation	3	2	2	2	2	11	Medium

Table 8: DREAD Threat Rating

5.5 Proposed Countermeasures and Implementing STRIDE Threat Model

The countermeasures of threats categorized in section 5.4 are provided in Table 9. In this section, the data flow in the cloud model is explained using the STRIDE threat modelling framework. This is important to understand the potential threats to data flow in the cloud model. This modelling also helps to understand the data flow from an attacker's perspective. The process of threat modelling is performed before deploying the cloud platform to identify potential threats. During modelling, elements of the system such as devices, data storage, data flow, and external entities are considered. Cloud threat modelling is shown in Figure 4. The cloud architecture is divided into zones where the authentication and authorization in each zone are performed separately. Then zones are separated by trust boundaries (dotted lines) to represent data transition from one source to another. As shown in Figure 5, the service zone and cloud gateway zone interact with the authentication controller of the cloud which is responsible for the authentication and authorization of users (admin and tenants). The field gateway zone interacts with the authentication controller and device zone and places all requests in a queue. The queue server interacts with devices that are responsible to handle the compute, storage, or network-related requests.

Category	Threat	Countermeasure
Spoofing	Spoofing	Authentication mechanism
Tampering	Forgery	Input validation mechanism
Repudiation	Data repudiation	Logging or auditing of record
Information Disclosure	Sniffing	Encrypting the data communication
Denial of service	DoS attack	Input validation mechanism
Elevation of Privilege	Code injection	No mitigation provided
Denial of Service	Interruption of Service	No mitigation provided
Elevation of Privilege	Lack of authorization	State-change requests mechanism

Table 9: STRIDE Generated Threats

The threat modelling report is generated based on the designed system. The report shows that there are 41 threats in the cloud model and how an attacker can attack the system. These threats are summarized into spoofing, forgery, DoS, data leakage, data repudiation, sniffing, interruption, impersonation, code injection, lack of authentication, and lack of authorization. The modelling tools not only depict potential threats but also often suggest countermeasures as shown in Table 9. From the measure results following are the publication trends observed.

#	Sub-categories of domain	Percentage
1	Data security	47%
2	Data leak	10%
3	Communication security	3%
4	User authentication	18%
5	Regulatory compliance	7%
6	Risk management	5%
7	Botnet attacks	10%

Table 10: Publication Trend

6 Conclusion

This study discussed privacy, security, and trust-related issues in the adoption of cloud computing platforms for the banking sector. An SLR is conducted to identify these challenges and mitigation methodologies. In addition, a survey from researchers in the field is conducted to find the latest challenges in the field of cloud computing. As a result of SLR, seven (7) unique threats are identified. Microsoft STRIDE threat modelling framework is used to further categorize this threat from the perspective of a cloud designer. This STRIDE model provides a data flow diagram that represents the flow of information among different components of the framework. This model helped to identify the threats in different components of the cloud platform, unlike the previous studies that target individual threats in a particular component of the platform. A comparison of threats identified from the SLR and threat modelling framework shows that the SLR lacks studies on repudiation attacks that are basic threats to data. In the future, a private cloud-based model is proposed for banking systems addressing different privacy, security, and trust-related issues in the banking sector. This model will help the users to take advantage of cloud computing power while keeping the lowest footprint of cyber-attacks.

References

1 M.Feridun and A. Özün, "Basel IV implementation: a review of the case of the European Union", Journal of Capital Markets Studies, vol. 4, no. 1, pp. 7–24, 2020, https://doi.org/10.1108/JCMS-04-2020-0006.

2 A. Didenko, "Cybersecurity regulation in the financial sector: prospects of legal harmonization in the European Union and beyond", Uniform Law Review, vol. 25, no. 1, pp. 125–167, 2020. https://doi.org/10.1093/ulr/unaa006.

3 L. Alhenaki, A. Alwatban, B. Alamri, and N. Alarifi, "A Survey on the Security of Cloud Computing," 2nd Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2019, pp. 1–7, 2019, doi: 10.1109/CAIS.2019.8769497.

4 P. J. Sun, "Security and privacy protection in cloud computing: Discussions and challenges," J. Netw. Comput. Appl., vol. 160, p. 102642, 2020, doi: 10.1016/j.jnca.2020.102642.

5 F. A. M. Ibrahim and E. E. Hemayed, "Trusted Cloud Computing Architectures for infrastructure as a service: Survey and systematic literature review," Comput. Secur., vol. 82, pp. 196–226, 2019, doi: 10.1016/j.cose.2018.12.014.

6 L. Zhao et al., "Research Gaps and trends in Cloud Computing: A systematic mapping study," Int. J. Cloud Comput., vol. 2, no. 4, 2014.

7 A. Esther Omolara et al., "State-of-The-Art in Big Data Application Techniques to Financial Crime: A Survey," Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 7, pp. 6–16, 2018.

8 A. Mahalle, J. Yong, X. Tao, and J. Shen, "Data Privacy and System Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure," Proc. 2018 IEEE 22nd Int. Conf. Comput. Support. Coop. Work Des. CSCWD 2018, pp. 75–80, 2018, doi: 10.1109/CSCWD.2018.8465318.

9 An Approach to Network and Application Security," Proc. - 3rd IEEE Int. Conf. Cyber Secur. Cloud Comput. CSCloud 2016 2nd IEEE Int. Conf. Scalable Smart Cloud, SSC 2016, pp. 1–6, 2016, doi: 10.1109/CSCloud.2016.18.

10 G. Uctu, M. Alkan, I. A. Dogru, and M. Dorterler, "Perimeter Network Security Solutions: A Survey," 3rd Int. Symp. Multidiscip. Stud. Innov. Technol. ISMSIT 2019 - Proc., 2019, doi: 10.1109/ISMSIT.2019.8932821.

11 S. Lehrig, H. Eikerling, and S. Becker, "Scalability, elasticity, and efficiency in cloud computing: A systematic literature review of definitions and metrics," QoSA 2015 - Proc. 11th Int. ACM SIGSOFT Conf. Qual. Softw. Archit. Part CompArch 2015, no. 1, pp. 83–92, 2015, doi: 10.1145/2737182.2737185.

12 M. Chiregi and N. Jafari Navimipour, "Cloud computing and trust evaluation: A systematic literature review of the state-of-the-art mechanisms," J. Electr. Syst. Inf. Technol., vol. 5, no. 3, pp. 608–622, 2018, doi: 10.1016/j.jesit.2017.09.001.

13 C. Okoli and K. Schabram, "A Guide to Conducting a Systematic Literature Review of Information Systems Research," SSRN Electron. J., vol. 10, no. 2010, 2010.

14 C. Okoli, "A guide to conducting a standalone systematic literature review," Commun. Assoc. Inf. Syst., vol. 37, no. 1, pp. 879–910, 2015, doi: 10.17705/1cais.03743.

15 B. Kitchenham, "Procedures for Performing Systematic Reviews," 2004. doi: 10.1145/3328905.3332505.

16 B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, "Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review," IEEE Access, vol. 8, pp. 120331–120350, 2020, doi:

10.1109/ACCESS.2020.3006358.

17 P. Vijayakumar et al., "MGPV: A novel and efficient scheme for secure data sharing among mobile users in the public cloud," Futur. Gener. Comput. Syst., vol. 95, pp. 560–569, 2019, doi: 10.1016/j.future.2019.01.034.

18 M. S. Das, A. Govardhan, and D. V. Lakshmi, "A classification approach for web and cloud based applications," Proc. - 2016 Int. Conf. Eng. MIS, ICEMIS 2016, 2016, doi: 10.1109/ICEMIS.2016.7745356.

19 E. M. Benhani, L. Bossuet, and A. Aubert, "The Security of ARM TrustZone in a FPGA-Based SoC," IEEE Trans. Comput., vol. 68, no. 8, pp. 1238–1248, 2019, doi: 10.1109/TC.2019.2900235.

20 A. Anitha, M. Varalakhshmi, A. Mary Mekala, Subashanthini, and M. Thilagavathy, "Secured cloud banking transactions using two-way verification process," Int. J. Civ. Eng. Technol., vol. 9, no. 1, pp. 531–540, 2018.

21 N. R. Parab, L. M. M. Colaco, and F. Coutinho, "Cloud based secure banking application," RTEICT 2017 - 2nd IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. Proc., vol. 2018-Janua, pp. 830–834, 2017, doi: 10.1109/RTEICT.2017.8256714.

22 R. K. Shyamasundar, N. V. N. Kumar, and P. Teltumde, "Realizing software vault on Android through information-flow control," Proc. - IEEE Symp. Comput. Commun., no. i, pp. 1007–1014, 2017, doi: 10.1109/ISCC.2017.8024657.

23 F. F. Alruwaili and T. A. Gulliver, "Secure migration to compliant cloud services: A case study," J. Inf. Secur. Appl., vol. 38, pp. 50–64, 2018, doi: 10.1016/j.jisa.2017.11.004.

24 V. Kumar, S. Kumar, and A. K. Gupta, "Real-Time detection of botnet behavior in cloud using domain generation algorithm," ACM Int. Conf. Proceeding Ser., vol. 12-13-Augu, pp. 1–3, 2016, doi: 10.1145/2979779.2979848.

25 E. Pakulova, A. Ryndin, and O. Basov, "Multi-path multimodal authentication system for remote information system," ACM Int. Conf. Proceeding Ser., pp. 10–13, 2019, doi: 10.1145/3357613.3357640.

26 A. M. Ximenes et al., "Implementation QR Code Biometric Authentication for Online Payment," IES 2019 - Int. Electron. Symp. Role Techno-Intelligence Creat. an Open Energy Syst. Towar. Energy Democr. Proc., pp. 676–682, 2019, doi: 10.1109/ELECSYM.2019.8901575.

27 S. Meean, Authentication Scheme Using Sparse Matrix in Cloud Computing, vol. 1, no. March. Springer International Publishing, 2018.

28 B. Tine, "PageVault: Securing Off-Chip Memory using Page-Based Authentication," 2017.

29 R. Bose, S. Chakraborty, and S. Roy, "Explaining the Workings Principle of Cloud-based Multi-factor Authentication Architecture on Banking Sectors," *Proc. - 2019 Amity Int. Conf. Artif. Intell. AICAI 2019*, pp. 764–768, 2019, doi: 10.1109/AICAI.2019.8701317.

30 D. Migdal, C. Johansen, and A. Jøsang, "DEMO: OffPAD - Offline personal authenticating device with applications in hospitals and e-banking," *Proc. ACM Conf. Comput. Commun. Secur.*, vol. 24-28-Octo, pp. 1847–1849, 2016, doi: 10.1145/2976749.2989033.

31 R. Wazirali, Z. Chaczko, and E. Chiang, "Steganographic authentication in cloud storage for mitigation of security risks," *Proc. - 25th Int. Conf. Syst. Eng. ICSEng 2017*, vol. 2017-Janua, pp. 451–458, 2017, doi: 10.1109/ICSEng.2017.61.

32 F. Reimair, C. Kollmann, and A. Marsalek, "Emulating U2F authenticator devices," *2016 IEEE Conf. Commun. Netw. Secur. CNS 2016*, no. Spc, pp. 543–551, 2017, doi: 10.1109/CNS.2016.7860546.

33 T. Y. Lin and C. S. Fuh, "Considerations of emerging cloud computing in financial industry and one-time password with valet key solution," *Proc. - 2016 16th IEEE Int. Conf. Comput. Inf. Technol. CIT 2016, 2016 6th Int. Symp. Cloud Serv. Comput. IEEE SC2 2016 2016 Int. Symp. Secur. Priv. Soc. Netwo*, pp. 724–731, 2017, doi: 10.1109/CIT.2016.81.

34 S. Ilankumaran and C. Deisy, "Multi-biometric authentication system using finger vein and iris in cloud computing," *Cluster Comput.*, vol. 22, pp. 103–117, 2019, doi: 10.1007/s10586-018-1824-9.

35 V. Vassilev, A. Phipps, M. Lane, K. Mohamed, and A. Naciscionis, "Two-factor authentication for voice assistance in digital banking using public cloud services," *Proc. Conflu. 2020 - 10th Int. Conf. Cloud Comput. Data Sci. Eng.*, pp. 404–409, 2020, doi: 10.1109/Confluence47617.2020.9058332.

36 I. Gordin, A. Graur, and A. Potorac, "Two-factor authentication framework for private cloud," *2019 23rd Int. Conf. Syst. Theory, Control Comput. ICSTCC 2019 - Proc.*, pp. 255–259, 2019, doi: 10.1109/ICSTCC.2019.8885460.

37 S. Asadi, M. Nilashi, A. R. C. Husin, and E. Yadegaridehkordi, "Customers perspectives on adoption of cloud computing in banking sector," *Inf. Technol. Manag.*, vol. 18, no. 4, pp. 305–330, 2017, doi: 10.1007/s10799-016-0270-8.

38 B. Odusote, O. Daramola, and M. Adigun, "Towards an extended misuse case framework for elicitation of cloud dependability requirements," *ACM Int. Conf. Proceeding Ser.*, pp. 135–144, 2018, doi: 10.1145/3278681.3278698.

39 H. Hassan, A. I. El-Desouky, A. Ibrahim, E. S. M. El-Kenawy, and R. Arnous, "Enhanced QoS-Based Model for Trust Assessment in Cloud Computing Environment," *IEEE Access*, vol. 8, pp. 43752–43763, 2020, doi: 10.1109/ACCESS.2020.2978452.

40 P. Li, J. Li, Z. Huang, C. Z. Gao, W. Bin Chen, and K. Chen, "Privacy-preserving outsourced classification in

cloud computing," *Cluster Comput.*, vol. 21, no. 1, pp. 277–286, 2018, doi: 10.1007/s10586-017-0849-9.

41 V. Kanimozhi and T. P. Jacob, "Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing," *ICT Express*, no. xxxx, 2020, doi: 10.1016/j.icte.2020.12.004.

42 A. Elzamly, B. Hussin, A. Samad, H. Basari, and C. Technology, "Classification of Critical Cloud Computing Security Issues for Banking Organizations: A Cloud Delphi Study," vol. 9, no. 8, pp. 137–158, 2016.

43 C. A. Ardagna, K. Ariyapala, M. Conti, C. M. Pinotti, and J. Stefa, "Anonymous end-to-end communications in adversarial mobile clouds," *Pervasive Mob. Comput.*, vol. 36, pp. 57–67, 2017, doi: 10.1016/j.pmcj.2016.09.001.

44 A. Mahalle, J. Yong, and X. Tao, "Insider threat and mitigation for cloud architecture infrastructure in banking and financial services industry," *Proc. 2019 IEEE 23rd Int. Conf. Comput. Support. Coop. Work Des. CSCWD 2019*, pp. 16–21, 2019, doi: 10.1109/CSCWD.2019.8791906.

45 D. D. Kankhare and A. A. Manjrekar, "A cloud based system to sense security vulnerabilities of web application in open-source private cloud IAAS," *2016 Int. Conf. Electr. Electron. Commun. Comput. Optim. Tech. ICEECCOT 2016*, pp. 252–255, 2017, doi: 10.1109/ICEECCOT.2016.7955225.

46 A. Mahalle, J. Yong, and X. Tao, "Protecting Privacy in Digital Era on Cloud Architecture for Banking and Financial Services Industry," *BESC 2019 - 6th Int. Conf. Behav. Econ. Socio-Cultural Comput. Proc.*, 2019, doi: 10.1109/BESC48373.2019.8963459.

47 O. Shkodina, I. Derid, and I. Zelenko, "DIGITAL TRANSFORMATION OF GLOBAL BANKING: CHALLENGES AND PROSPECTS," *Financ. Credit Act. Probl. Theory Pract.*, vol. 30, no. 3, pp. 45–51, 2019.

48 D. Tribedi, D. Sadhukhan, and S. Ray, *Cryptanalysis of a Secure and Privacy Preserving Mobile Wallet Scheme with Outsourced Verification in Cloud Computing*, vol. 1031, Springer Singapore, 2019.

49 R. Saxena, M. Jain, A. Kushwah, and D. Singh, "An Enhanced Parallel Version of RSA Public Key Crypto Based Algorithm Using OpenMP," *ACM Int. Conf. Proceeding Ser.*, pp. 37–44, 2017, doi: 10.1145/3136825.3136866.

50 K. Tyagi, A. Mishra, and M. Singh, "A novel cryptographic data security approach for banking industry to adopt cloud computing," *Int. J. Recent Technol. Eng.*, vol. 7, no. 5, pp. 356–361, 2019.

51 O. P. Jena, A. Tripathy, S. Swagatam, S. Rath, and A. R. Tripathy, "Dual encryption model for preserving privacy in cloud computing," *Adv. Math. Sci. J.*, vol. 9, no. 9, pp. 6667–6678, 2020, doi: 10.37418/amsj.9.9.24.

52 A. Salim, S. Tripathi, and R. K. Tiwari, "Applying Geo-Encryption and attribute based encryption to implement secure access control in the cloud," *Int. J. Comput. Networks Commun.*, vol. 11, no. 4, pp. 121–135, 2019, doi: 10.5121/ijcnc.2019.11407.

53 K. Suveetha and T. Manju, "Ensuring confidentiality of cloud data using homomorphic encryption," *Indian J. Sci. Technol.*, vol. 9, no. 8, pp. 1–7, 2016, doi: 10.17485/ijst/2016/v9i8/87964.

54 S. Dhal and V. Bhuwan, "Cryptanalysis and improvement of a cloud based login and authentication protocol," *Proc. 4th IEEE Int. Conf. Recent Adv. Inf. Technol. RAIT 2018*, pp. 1–6, 2018, doi: 10.1109/RAIT.2018.8388988.

55 B. B. Kırlar, S. Ergün, S. Z. Alparslan Gök, and G. W. Weber, "A game-theoretical and cryptographical approach to crypto-cloud computing and its economical and financial aspects," *Ann. Oper. Res.*, vol. 260, no. 1–2, pp. 217–231, 2018, doi: 10.1007/s10479-016-2139-y.

56 D. Gozman and L. Willcocks, "The emerging Cloud Dilemma: Balancing innovation with cross-border privacy and outsourcing regulations," *J. Bus. Res.*, vol. 97, no. June 2017, pp. 235–256, 2019, doi: 10.1016/j.jbusres.2018.06.006.

57 W. K. Hon and C. Millard, "Banking in the cloud: Part 1 – banks' use of cloud services," *Comput. Law Secur. Rev.*, vol. 34, no. 1, pp. 4–24, 2018, doi: 10.1016/j.clsr.2017.11.005.

58 W. K. Hon and C. Millard, "Banking in the cloud: Part 2 – regulation of cloud as 'outsourcing,'" *Comput. Law Secur. Rev.*, vol. 34, no. 2, pp. 337–357, 2018, doi: 10.1016/j.clsr.2017.11.006.

59 W. K. Hon and C. Millard, "Banking in the cloud: Part 3 – contractual issues," *Comput. Law Secur. Rev.*, vol. 34, no. 3, pp. 595–614, 2018, doi: 10.1016/j.clsr.2017.11.007.

60 S. Pokharel, K. K. R. Choo, and J. Liu, "Mobile cloud security: An adversary model for lightweight browser security," *Comput. Stand. Interfaces*, vol. 49, pp. 71–78, 2017, doi: 10.1016/j.csi.2016.09.002.

61 M. Ramachandran and V. Chang, "Towards performance evaluation of cloud service providers for cloud data security," *Int. J. Inf. Manage.*, vol. 36, no. 4, pp. 618–625, 2016, doi: 10.1016/j.ijinfomgt.2016.03.005.

62 W. Zheng, L. Yan, C. Gou, and F. Y. Wang, "Federated meta-learning for fraudulent credit card detection," *IJCAI Int. Jt. Conf. Artif. Intell.*, vol. 2021-Janua, pp. 4654–4660, 2020, doi: 10.24963/ijcai.2020/642.

63 H. Huang, X. Chen, Q. Wu, X. Huang, and J. Shen, "Bitcoin-based fair payments for outsourcing computations of fog devices," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 850–858, 2018, doi: 10.1016/j.future.2016.12.016.

64 A. Elzamly *et al.*, "A new conceptual framework modelling for cloud computing risk management in banking organizations," *Int. J. Grid Distrib. Comput.*, vol. 9, no. 9, pp. 137–154, 2016, doi: 10.14257/ijgdc.2016.9.9.13.

65 T. A. Mohammed and A. B. Mohammed, "Security

architectures for sensitive Data in Cloud Computing," in *Proceedings of the 6th International Conference on Engineering & MIS 2020*, 2020, pp. 1–6, doi: 10.1145/3410352.3410828.

66 T. Daisy Premila Bai, A. Vimal Jerald, and S. Albert Rabara, "An adaptable and secure intelligent smart card framework for internet of things and cloud computing," *Adv. Intell. Syst. Comput.*, vol. 654, pp. 19–28, 2018, doi: 10.1007/978-981-10-6620-7_3.

67 M. Bélair, S. Laniepce, and J. M. Menaud, "Leveraging kernel security mechanisms to improve container security: A survey," *ACM Int. Conf. Proceeding Ser.*, 2019, doi: 10.1145/3339252.3340502.

68 M. Auxilia and K. Raja, "Knowledge based security model for banking in cloud," *ACM Int. Conf. Proceeding Ser.*, vol. 25-26-Augu, 2016, doi: 10.1145/2980258.2980364.

69 H. Alsaghier, "A secure mobile commerce framework based on community cloud," *Int. J. Inf. Comput. Secur.*, vol. 9, no. 1–2, pp. 100–113, 2017, doi: 10.1504/IJICS.2017.082841.

70 S. Biswas and A. Roy, "An Intrusion Detection System Based Secured Electronic Service Delivery Model," *Proc. 3rd Int. Conf. Electron. Commun. Aerosp. Technol. ICECA 2019*, pp. 1316–1321, 2019, doi: 10.1109/ICECA.2019.8822016.

71 H. Hui, D. McLernon, and A. Zaidi, "Design of the Security Mechanism for a BPO Cloud Computing Platform," *Proc. IEEE Int. Conf. Softw. Eng. Serv. Sci. ICSESS*, vol. 2018-Novem, pp. 1092–1095, 2019, doi: 10.1109/ICSESS.2018.8663713.

72 M. Sumathi and S. Sangeetha, "Scale-based secured sensitive data storage for banking services in cloud," *Int. J. Electron. Bus.*, vol. 14, no. 2, pp. 171–188, 2018, doi: 10.1504/IJEB.2018.094863.

73 A. Roskladka, N. Roskladka, G. Kharlamova, and R. Baglai, "Cloud based architecture of the core banking system," *CEUR Workshop Proc.*, vol. 2393, pp. 316–331, 2019.

74 P. Aufner, "The IoT security gap: a look down into the valley between threat models and their implementation," *Int. J. Inf. Secur.*, vol. 19, no. 1, pp. 3–14, 2020, doi: 10.1007/s10207-019-00445-y.

75 A. Honkaranta, T. Leppanen, and A. Costin, "Towards Practical Cybersecurity Mapping of STRIDE and CWE - A Multi-perspective Approach," *Conf. Open Innov. Assoc. Fruct*, vol. 2021-May, pp. 150–159, 2021, doi: 10.23919/FRUCT52173.2021.9435453.

76 J. B. F. Sequeiros, F. T. Chimuco, M. G. Samaila, M. M. Freire, and P. R. M. Inácio, "Attack and System Modeling Applied to IoT, Cloud, and Mobile Ecosystems: Embedding Security by Design," *ACM Comput. Surv.*, vol. 53, no. 2, 2020, doi: 10.1145/3376123.

77 A. Shostack, *Threat Modeling: Designing For Security*. John Wiley & Sons, 2014.