Enhancing Trust in Peer-to-Peer Data Transfer: Implementing Zero-Knowledge Succinct Proofs and a Trusted Factor for Robust RC-based P2P Systems

Anjila Neupane[*]
Southeast Missouri State University, Cape Girardeau, USA
Indranil Roy[†]
Southeast Missouri State University, Cape Girardeau, USA.
Reshmi Mitra[‡]
Southeast Missouri State University, Cape Girardeau, USA
Bidyut Gupta [§]
Southern Illinois University; Carbondale, IL, USA.
Narayan C. Debnath [¶]
Eastern International University, Vietnam.

Abstract

Peer-to-peer (P2P) networks are a class of network systems distinguished by their capacity for large-scale distributed information sharing. In this context, a number of novel P2P topologies are put forth, including the interest-based Residue Class (RC) P2P networks, which are non-DHT. The RC-based P2P networks are open, dispersed, and anonymous, making them susceptible to a number of security issues. Because RC-based P2P networks lack a centralized authority to control the nodes that constantly join and exit the network, trust verification is a challenging problem. In this research, we offer a trust model designed for RC-based P2P networks. To build trust, we employ a Trust Factor (TF) in conjunction with the Zero-Knowledge Proof (ZKP) idea. The foundation of the model is the trust mechanism that allows nodes to improve and establish their reputation within the network. By effectively recognizing malicious nodes inside the RC-based P2P network and mitigating the likelihood of an attack on the decentralized system, the trust model ensures secure file-sharing and communication.

1 Introduction

Peer-to-peer (P2P) overlay networks are commonly employed in distributed systems because of their ability to provide computational and data resource sharing in a scalable, self-organizing, distributed manner. Unstructured and structured P2P networks are the two subtypes of P2P networks. In unstructured systems, peers can be grouped in any topology at random [6]. It takes flooding to look up data. “Churn” — the challenges caused by peers joining and leaving the system frequently—is well managed in unstructured systems. Nevertheless, this reduces the vital flexibility and efficacy of data querying. There is no guarantee on lookups in unstructured networks. Structured overlay networks, on the other hand, provide deterministic boundaries for data discovery. Based on a distributed data structure that genuinely permits deterministic data search behavior, they develop scalable network overlays.

A recent development in the architecture of structured overlay systems is the use of distributed hash tables (DHTs) [16, 25, 44]. According to [16, 25, 26, 44, 48], overlay designs of this kind can offer effective, adaptable, and robust services. On the other hand, keeping DHTs while handling the churn issue gets costly. Designing an efficient data query service necessitates a major shift. Creating hybrid systems has been the subject of several noteworthy articles in this field [14, 35, 39, 49]. The aforementioned studies endeavor to integrate the advantages of both structured and unstructured frameworks. However, these efforts come with a unique mix of benefits and drawbacks [2].

There has also been much interest in a non-DHT-based structural design method that is interest/resource driven [18, 22]. In addition to aiming to reduce churn management complexity, it provides the advantages of DHT-based systems. Our paper presents a non-DHT fog computing architecture that is built on interest/resource and publish/subscribe mechanisms. This

[*] Department of Computer Science, Southeast Missouri State University, Cape Girardeau, MO. Email: : aneupane4s@semo.edu

[†] Department of Computer Science, Southeast Missouri State University, Cape Girardeau, MO. Email: : aneupane4s@semo.edu

[‡] Department of Computer Science, Southeast Missouri State University, Cape Girardeau, MO. Email: : aneupane4s@semo.edu

[§] School of Computing, Southern Illinois University; Carbondale, IL. Email: bidyut@cs.siu.edu.

[¶] School of Computing and Information Technology, Eastern International University, Vietnam. Email: NdebnathC@gmail.com .

architecture facilitates efficient resource sharing for sensor data processing. In designing the architecture, we considered the non-DHT-based interest/resource-based architecture suggested in [18, 22].

Due to the lack of centralized authority to control the frequent joining and departing of nodes, peer-to-peer (P2P) distributed trust verification is a complicated problem [3]. The trade-offs between security, performance, and cost are substantial. The network may experience a considerable load as more nodes are added, marking each one as authentic. Second, devastating attacks like replay, sybil, and eclipse attacks—in which the adversary produces a large number of malicious peers—can occur on P2P networks. Furthermore, the processing and bandwidth capacity of these networks is constrained, which makes it challenging to deploy a resource-intensive protocol for defense and mitigation. It becomes very difficult to integrate traditional Public-key Infrastructure (PKI) because of these problems. In general, the dispersed network necessitates that users authenticate one another in a scalable, secure, and effective way. P2P networks are open and anonymous, which makes it simple for malevolent users to enter the network and cause havoc by introducing fake content [7]. Peers find it uncomfortable to initiate contact with unfamiliar users in such a setting until they are seen as trustworthy. Credibility can be offered through the use of a reputation system. Many experiments on reputation systems to simulate peers' prior behavior have been conducted in recent years [1], [24], [47], [41], [52], [53], [28], [40], [12], [32], [5], [46], [8], [9], and [45]. However, there is still work to be done in integrating them into the actual system. The most effective example of Google's reputation system, PageRank [34], determines a page's reputation based on how popular it is on the internet. The quantity of links pointing to the page and the popularity of the pages from which the connections originate are the two metrics used to gauge popularity. Reputation systems have been developed for peer ranking based on a similar principle, where the most reputable peer is deemed to be the most trustworthy [24], [52], [53], and [40]. In any such system, the network as a whole usually builds the consensus. There are four main, fundamental issues with these reputation systems.

Finding a balance between anonymity vs. trust [43] is a significant problem in P2P networks. Anonymity is a highly wanted feature for privacy reasons, allowing users to communicate without disclosing their identities or sensitive information. Users are shielded from targeted attacks, censorship, and spying as a result. However, this level of anonymity allows malicious actors to disrupt the system in a covert manner without triggering any detection mechanism. However, trust necessitates identification confirmation or tracking past behavior, both of which put users' anonymity at risk. Building trust in a highly anonymous network is extremely challenging, which makes it harder to hold malicious nodes responsible and boosts network-level attacks such as spamming and the spread of false information. However, a reliance on trust sometimes means relying on reputation or identity verification systems, which can compromise user privacy. Thus, it can be difficult to strike the right balance between these two opposing objectives in P2P networks.

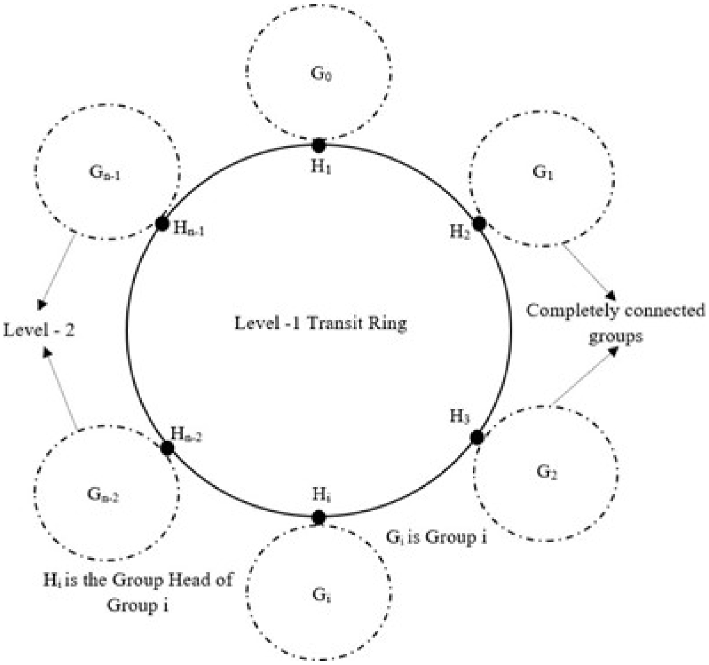


Figure 1: Sequence diagram for an encrypted message sent from sender to receiver after successfully verifying the receiver [11].

Lightweight cryptography using Zero Knowledge Proofs (ZKP) offers a compelling solution to address the above challenges. ZKP allows a prover to demonstrate to a verifier that a certain statement such as the legitimacy of a node is true, without revealing any information beyond the truth of the statement itself. This provides a mechanism for establishing trust while preserving user anonymity which is a challenging balancing act in P2P network. Moreover, ZKPs are beneficial in minimizing computational overhead and communication costs, essential for the effective operation of resource-constrained P2P networks. Furthermore, the unique aspect of ZKPs is to provide non-interactive proofs that are succinct and efficient, requiring minimum interaction between prover and verifier, reducing network latency, and speeding up the data transfer process.

The authors of [11] have presented a ZKP-based protocol that is lightweight, safe, and efficient for building and preserving trust between anonymous peers and group chiefs in a P2P network during the data transfer phase. The communication is started by the sender group head asking the recipient node to complete a one-step challenge (such SHA-ing a random number). The sender uses the unique solution they have received as a nonce to encrypt the message and send it to the recipient. Since the recipient node is the only one with the decryption key, only it can decrypt the message. It basically carries out a safe key transfer procedure together with a symmetric encryption algorithm. Without jeopardizing any private data, the sender node can easily create an alternative compact problem statement by altering the mathematical operation or random number. Additionally, without the intervention of a third party, the protocol can be performed numerous times until the verifier is satisfied with the prover's reliability.

When a recipient node fails to react within the predefined timeout period or responds incorrectly to the sender's challenge, it is classified as 'corrupt'. As a punishment and deterrent for breaking the protocol, nodes that have been flagged as corrupt are essentially barred from participating in any further phases of data transfer. The network's integrity is maintained by this continuous detection mechanism, which shields it from nodes that can jeopardize the security operation of the system.

By balancing user anonymity and the reliability of group head nodes, this protocol tackles the challenging problem of distributed trust verification in peer-to-peer networks. It is perfect for P2P networks with limited resources since it requires less interaction, which lowers communication and computing overhead. Furthermore, continuous trust verification is suggested by this method. This removes presumptions regarding intrinsic reliability and hence lowers the risk of assaults. It strengthens network security and protects user privacy by making our approach a reliable and scalable trust verification technique.

According to the authors in [11], in the worst case, the number of hops needed rises as 2k+3 (where k is the maximum number of puzzles the network administrator has set),and the ZKP puzzle transfer is only generated during the data transfer phase. This results in a lag in the data transfer process. Another problem with the security approach described by Deverasetti et al. [11] is that it has very strict policies that are not tolerant in the slightest. For example, a recipient node is labeled as "corrupt" if it fails to respond to a challenge from the sender within the predetermined timeout period or if it responds incorrectly. In this paper, we propose a regular maintenance approach to address these issues and make the policies more tolerant. We incorporate a Trust Factor (TF) that is updated each time the nodes exchange ZKP challenges, along with the same ZKP-based security approach as in [11]. Basically, this TF will allow the nodes/peers to self-correct in case drastic ; we'll go into more depth about this in section 3. Moreover, this approach suggests continuous trust verification, which reduces the likelihood of attacks by eliminating assumptions about intrinsic reliability.

This makes our methodology a scalable and trustworthy trust verification method, enhancing network security and safeguarding user privacy. This paper has four main sections. In Section 2, we give the overview of the previously proposed RC-based P2P network and the background on Zero Knowledge Proof (ZKP). Followed by in section 3 we propose our ZKP Maintenance Protocol and the secured data-lookup . Model evaluation and discussion is part of Section 4. We are concluding with the highlights of our work in Section 5.

2 Preliminaries

2.1 RC-Based P2P Network [19]

Here, we have taken into consideration some of the first results of an RC-based low diameter two level hierarchical structured P2P network [19, 21, 30]. We provide a structured design for an interest-based peer-to-peer system in this section. We will use the following notations and their meanings to define the architecture.

Definition 1: We define a resource as a tuple $<$ Resi, $V >$, where Resi denotes the type of a resource and V is the value of the resource. Note that a resource can have many values.

Definition 2: Let S be the set of all peers in a peer-to-peer system. Then

$$S = \{P_{R_i}\} \quad (0 \leq i \leq n-1)$$

where P_{R_i} denotes the subset consisting of all peers with the same resource type *Resipeer* among the peers in P_{R_i} to join the system. We call H_i as the group-head of group G_i formed by the peers in the subset P_{R_i}. We now describe our proposed architecture suitable for an interest-based peer-to-peer system. Generalization of the architecture is considered in [21]. We use the following notations along with their interpretations while we define the architecture.

2.1.1 Two Level Hierarchy

It is a two-level overlay architecture and at each level structured networks of peers exist. It is explained in detail below.

1. At level-1, we have a ring network consisting of the peers H_i $(0 \leq i \leq n-1)$. The number of peers on the ring is n, which is also the number of distinct resource types. This ring network is used for efficient data lookup, and so we name it the transit ring network.

2.At level-2, there are n completely connected networks (groups) of peers. Each such group, say G_i, is formed by the peers of the subset PR_i $(0 \leq i \leq n-1)$, such that all peers (PR_i) are directly connected (logically)

3. Every group is also going to have a secondary group head G_{sh} to maintain a fault-tolerant architecture. The secondary group head is going to be the next highest logical address afterAfter the group head, an address will be assigned. For example, in a network of 10 different resource types, for group 0, G_0^h will be the group head and G_0^{sh2} will be the secondary group head.

4. Each peer in the network maintains a Information Resource Table (IRT) that consists of n number of tuples.

* The group heads will have a tuple of the form <Resource Type, Resource Code, Group Head public Key>for other group heads and <Peer Logical Address, Peer public Key>for the other peers present in their respective group. The Group Head Logical Address are assigned according to the proposed logical address assignment algorithm proposed in [23] and the public key of the group heads or the peers are exchanged when they are joining the network and the IRT is updated and broadcasted

in the network. Also, Resource Code is the same as the group head logical address. article amsmath

The peers P_i, who are not group heads but belong to a group G_i (where $P_i \in G_i$), will have the following tuples:

- $\langle$Resource Type, Resource Code, Group Head Public Key$\rangle$ for the group head of G_i.
- $\langle$Peer Logical Address, Peer Public Key$\rangle$ for the other peers present in G_i.

5.Any communication between a peer $G_{x,i} \in G_x$ and $G_{y,j} \in G_y$ takes place only through the corresponding group heads H_x and H_y.

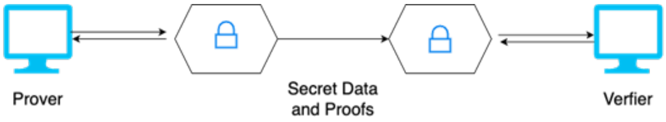


Figure 2: Example of a simple ZKP Protocol.

The proposed architecture is shown in Figure 1. The assignment of the logical addresses is described in [19].

2.1.2 Salient Features of Overlay Architecture

We summarize the salient features of this architecture.

1. It is a hierarchical overlay network architecture consisting of two levels; at each level the network is a structured one.

2. Use of modular arithmetic allows a group-head address to be identical to the resource type owned by the group. We will show in the following section the benefit of this idea from the viewpoint of achieving reasonably very low search latency.

3. Number of peers on the ring is equal to the number of distinct resource types, unlike in existing distributed hash table-based works some of which use a ring network at the heart of their proposed architecture [26].

4. The transit ring network has the diameter of n/2. Note that in general in any P2P network, the total number of peers $N >> n$.

5. Each overlay network at level 2 is completely connected. That is, in graph theoretic term it is a complete graph consisting of the peers in the group. So, its diameter is just

1. Because of this smallest possible diameter (in terms of number of overlay hops) the architecture offers minimum search latency inside a group.

2.2 Assurance of Trust in Peer-to-Peer Networks

Managing trust is a crucial element in peer-to-peer (P2P) networks, particularly when it comes to secure data sharing. Trust-based systems are key in maintaining the integrity, privacy, and accessibility of data within P2P networks. Balfe et el. suggested a framework for trusted computing to improve security in P2P networks. Their strategy involves using trusted computing technologies to create a secure base for P2P interactions. By combining trusted platform components and secure boot processes, they show how it's possible to ensure secure communication and data transfer in P2P networks [3].

Selcuk et el. introduced a system for managing trust in P2P networks based on reputation. This system uses the reputation of nodes to gauge their reliability. They highlight the significance of reputation management in P2P networks and offer a detailed framework that includes trust calculation and decision-making processes for effective trust assessment [38].

Zhao et el. tackled the challenge of verifying results and scheduling in P2P grids, focusing on grid computing settings where nodes are spread across different locations. They developed a scheduling algorithm that takes into account both the reputation of nodes and the accuracy of their reported data. Their work on this topic is titled ”Result Verification and Trust-Based Scheduling in P2P Grids” [51].

Frahat et el. introduced a secure and scalable approach to managing trust in IoT P2P networks. They recognized the distinct features and security issues of IoT environments and proposed a framework that guarantees secure communication and collaboration among IoT devices. Their approach includes trust evaluation, reputation management, and access control to build a secure and reliable IoT P2P network [13].

Hao et el. aimed to improve the reliability of P2P networks by incorporating blockchain technology. They suggested a blockchain-enhanced P2P topology that allows for quick and dependable information dissemination. The addition of trust mechanisms further enhances the reliability and trustworthiness of the P2P network [37].

2.3 Zero-Knowledge Proof (ZKP)

Zero-knowledge proofs (ZKP) are fundamental and powerful tools in cryptography. Zero-Knowledge Proof (ZKP) protocols are designed to assist provers in persuading verifiers that they possess certain knowledge, often confidential, while maintaining the integrity of the knowledge during the verification process (zero-knowledge) as shown in figure 2. Since its first introduction by Goldwasser et el. in [15], the notion of ZKP has been used in several authentication and identity systems.

A ZKP system is an interactive protocol in which the prover and the verifier communicate with each other for a predetermined number of rounds. If the assertion is true at the conclusion of these discussions, the verifier has to be persuaded of it. On the other hand, there is a good chance the verifier will find the lie if the assertion is not true. Three movements, or three communications named commitment, challenge, and answer, comprise each round. The statement to be proven is initially generated by the prover and sent to the verifier as a first message, or commitment. Next, a challenge is selected at random by the verifier and forwarded to the prover. Ultimately, the prover delivers the response to the verifier after computing it in light of the challenge.

A zero-knowledge proof is a demonstration that reveals nothing beyond the truth of a statement. Here, ”proof” refers not to the traditional mathematical concept but to an interactive protocol where one party (the prover) convinces another party (the verifier) of the truth of an argument. In a zero-knowledge proof, the prover shows they know a secret without disclosing it. Research in zero-knowledge proofs has been driven by authentication systems where one party wants to prove its identity to another using secret information (such as a password) without revealing the secret itself. This is known as a ”zero-knowledge proof of knowledge.” While passwords are often too small or not sufficiently random for zero-knowledge proofs of knowledge in many systems, the underlying principle is still highly significant.

ZKPs have been crucial in maintaining privacy and security within peer-to-peer (P2P) networks. Numerous studies have been conducted to implement ZKPs in P2P networks for secure communication. Danezis and Diaz introduced SybilInfer, a system that leverages social network analysis to detect malicious entities. ZKPs are utilized to improve the reliability of detection and bolster the security of P2P networks [10].

Lu et al. have examined the use of ZKPs for authentication in anonymous P2P networks. The study focuses on the development and implementation of a pseudo-trust system through zero-knowledge authentication [29].

Pop et al. have looked into the application of ZKPs to enhance privacy in energy transactions on the blockchain. The research suggests a scheme that guarantees privacy while ensuring the integrity of energy-related transactions [36].

X Sun et al. offer a comprehensive overview and analysis of ZKPs in blockchain applications. The review covers various topics, including the different types of ZKPs and their potential uses and challenges within the blockchain environment [42].

Yang and Li introduce a digital identity management system using ZKPs within a blockchain framework. The work proposes a secure and efficient method for managing digital identities while safeguarding privacy [50].

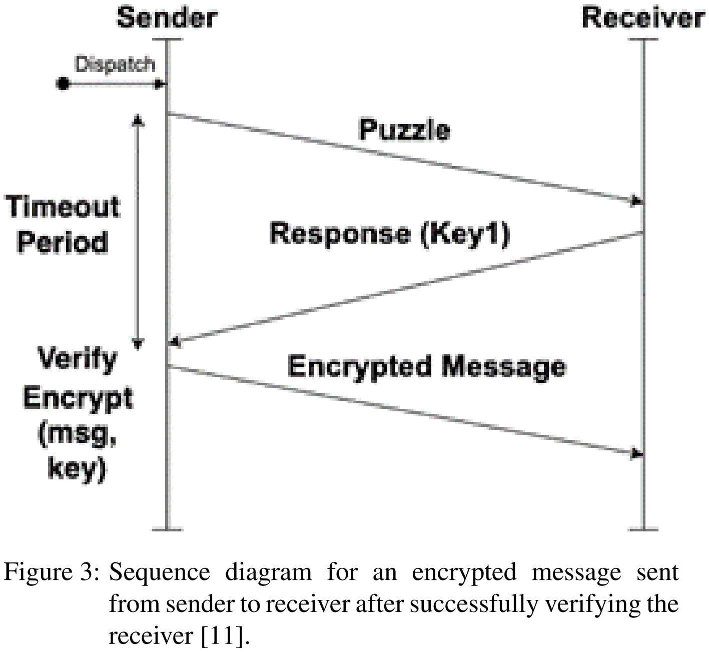


Figure 3: Sequence diagram for an encrypted message sent from sender to receiver after successfully verifying the receiver [11].

Harikrishnan and Lakshmy explore the application of ZKPs for secure payments in distributed networks. The authors suggest a scheme that ensures the confidentiality and integrity of digital service payments while maintaining anonymity [17].

Major et el. present an authentication protocol based on chaos theory and ZKPs. The paper introduces a new method to enhance security and privacy in authentication protocols [31]. Kosba et el. discuss the development of scalable ZKPs without a trusted setup. The work introduces a construction known as zk-STARKs, which provides an efficient and scalable solution for ZKPs [27].

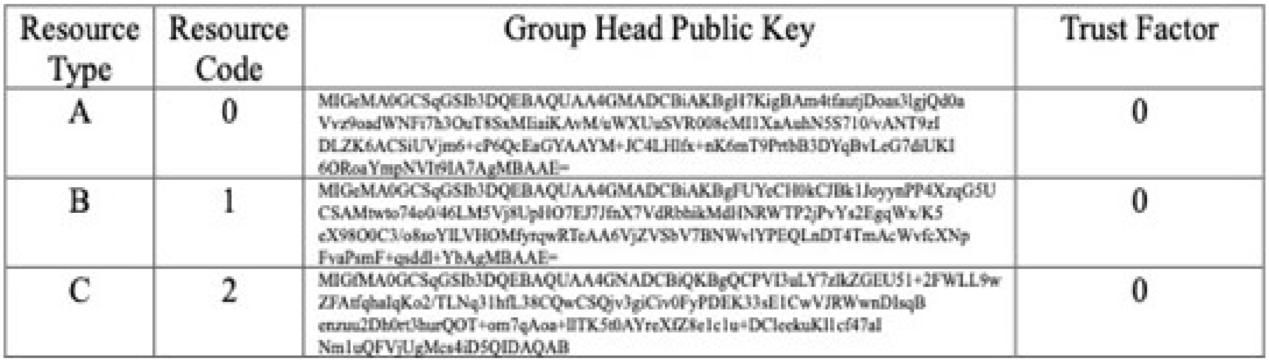
Ben-Sasson et el. concentrate on the creation of scalable ZKPs with no trusted setup. The paper introduces a construction called zk-STARKs, which offers a highly efficient and scalable approach to ZKPs [4].

One of the most compelling uses of zero-knowledge proofs within cryptographic protocols is to ensure honest behavior while maintaining secrecy. The idea is to require a user to prove that their actions are correct according to the protocol. Because of the soundness property, we know the user must act honestly to provide a valid proof. Due to the zero-knowledge property, the user does not compromise the privacy of their secrets during the proof process.

For example, in [11] the authors have incorporated the concept of ZKP. Irrespective of the intricacy of the proposition being proved or the amount of data involved, the authors have employed succinct proof that is very verifiable.

A result, in comparison to traditional NP verification, they need less processing complexity. They are specifically chosen to minimize communication and processing overhead. Furthermore, in order to minimize communication between the prover and verifier, the protocol is intended to assure minimal interactions. chosen to minimize communication and processing overhead. Furthermore, in order to minimize communication between the prover and verifier, the protocol is intended to assure minimal interactions. Because of this, the issue formulation is appropriate for the P2P trust verification context, which has limited resources. The sender group head node suggests a one- step challenge for creating proof and building confidence, such as SHA-256 hashing a random integer.

It is simple to alter this random number in order to provide a fresh challenge for every hop and produce a fresh verification key. In response to this difficulty, the receiver node—which is also the group head—develops a special method that can serve as a nonce, a number that is only used once to make sure that previous messages are not repeated in replay attacks. They transfer the message to the following hop in the network until it reaches its intended destination, after utilizing ZKPs to confirm the group head node’s reliability. It eliminates any presumptions that a peer is inherently trustworthy by ongoing trust verification. Rather, every node must demonstrate and earn its authenticity and integrity, which lessens assaults from corrupted nodes via replay and sybil, among other methods.



Resource Type	Resource Code	Group Head Public Key	Trust Factor
A	0	MIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgH7KigBAm4tfautjDoas3lgjQd0a Vvz9oadWNFi7h3OuT8SxMIiaiKAvM/uWXUuSVR008cMI1XaAuhN5S710/vANT9zl DLZK6ACSiUVjm6+cP6QcEaGYAAYM+JC4LHlfx+nK6mT9PrtbB3DYqBvLeG7diUKI 6ORoaYmpNVIt9IA7AgMBAAE=	0
B	1	MIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgFUYeCH0kCJBk1JoyynPP4XzqG5U CSAMtwto74o0/46LM5Vj8UpHO7EJ7JfnX7VdRbbikMdHNRWTP2jPvYs2EgqWx/K5 eX98O0C3/o8soYILVHOMfyrqwRTeAA6VjZVSbV7BNWvlYPEQLnDT4TmAcWvfcXNp FvaPsmF+qsddl+YbAgMBAAE=	0
C	2	MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCPVI3uLY7zlkZGEU51+2FWLL9w ZFAtfqhalqKo2/TLNq31hfL38CQwCSQjv3giCiv0FyPDEK33sE1CwVJRWwnDIsqB enzuu2Dh0rt3hurQOT+om7qAoa+lITK5t0AYrcXfZ8e1c1u+DCleckuKI1cf47al Nm1uQFVjUgMcs4iD5QIDAQAB	0

Figure 4: IRT example with 3 resource types

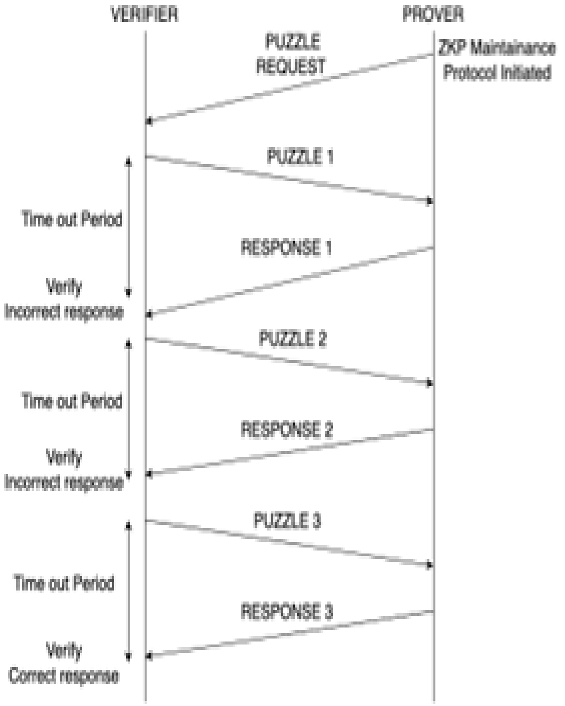


Figure 5: Sequence diagram for successful trust verification between Prover and Verifier

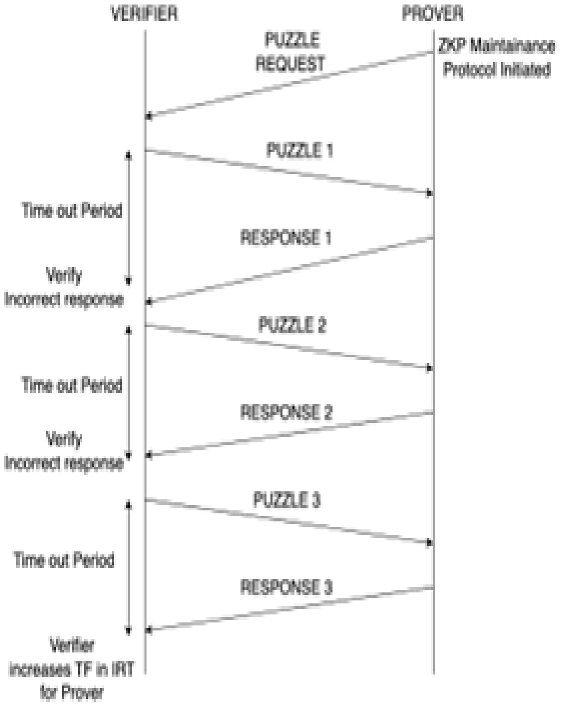


Figure 6: Sequence diagram for response lost during trust verification between Prover and Verifier

The ZKP puzzle transmission is only created during the data transfer phase, and in the worst scenario, the number of hops required increases as 2k+3 (where k is the maximum number of puzzles the network administrator has chosen), according to the authors in [11]. The data transfer procedure lags as a result. The highly rigorous and non-tolerant principles of the security method outlined by Deverasetti et el. [11] provide another issue. For instance, a receiving node is flagged as ”corrupt” if it answers erroneously or does not answer to a challenge from the sender within the allotted delay period.

As a result, we suggest a routine maintenance strategy in the section that follows to deal with these problems and improve the policies' tolerance. We implement the same ZKP-based security method as in [11], coupled with an updated Trust Factor (TF) every time the nodes exchange ZKP challenges. In essence, if something goes wrong, this TM will let the nodes/peers self-correct. Additionally, this method proposes ongoing trust validation, which lessens the probability of assaults by dispelling the notion of inherent dependability. As a result, our technique improves network security and protects user privacy while being scalable and reliable for trust verification.

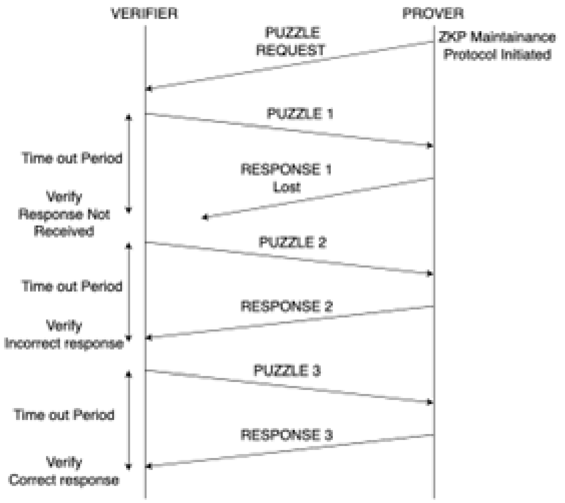


Figure 7: Sequence diagram for trust verification between Prover and Verifier where Prover is found to be potentially malicious

Algorithm 1 ZKP Maintenance Protocol

```
 1: Counter = 0
 2: Gh the Prover initiates the ZKP maintenance protocol
 3: Gh unicasts challenge request Puzreq to Verifier   (Verifier → Gh, Gh and Gsh)
 4: Verifier, after receiving Puzreq, generates PuzV and unicasts it to Gh$_{i+1}$
 5: Verifier waits for Tout   (Tout is the timeout set by the network administrator)
 6: Gh solves PuzV and responds with RePuzV to Verifier
 7: if (RePuzV is true) and (verified by Verifier) and (within TPout) then
 8:     if TF of Prover = 0 then
 9:         No change in TF is made by the Verifier in IRT
10:     else
11:         TF is decreased by 1 by the Verifier in IRT
12:         Broadcast it to other group heads using IRT
13:     end if
14: else
15:     if Counter ¡ 3 then
                                                  (Counter = Max
        TF value set by the network administrator)The respective
        Group Head re-initiates Step 6 Counter = Counter + 1
16:18:  else
19:         Verifier increases the TF for Gh in IRT by 1
20:         Broadcast it to other group heads using IRT
21:         Other group heads update their IRT
22:         if TF for Gh == 3 then
23:             Gh$_i$ is marked as malicious and removed from the network
                and broadcasted updated IRT to all other group heads
24:             The Gsh of Gi is made the new Gh and the next highest
                logical address after Gh$_i$ is made the new Gsh
25:         end if
26:     end if
27: end if
```

3 Zero-Knowledge Succinct Proofs and a Trusted Factor for RC-based P2P

In this section we present the regular maintenance strategy that every group head in the RC-based P2P network is going to use to maintain the trust in the network. In this scenario, we propose of including a new column in the Information Resource Table (IRT) mentioned in section 2.1.1, this column will be the Trust Factor (TF) as shown in figure 4 as an example, for say group head of group 0 i.e. Gh with 3 different resource types. The TF will be range from 0-3 or some other maximum value as determined by the network designer. The score ranges from '0' being the most trusted, '3' being extremely malicious and mildly suspicious for intermediary values. Initially all the group heads will be assigned with the TF 0. Every group head has to initiate the regular ZKP maintenance protocol within a certain time period as determined by the network designer. In the regular ZKP maintenance protocol, the group head initiating it, will be acting as the prover and the group heads adjacent to it as well as the secondary group head of that particular group will be serving as the verifier.

Algorithm 2 Secured Data Look-up and Transfer Protocol for RC-based P2P Network

```
 1: Gx initiates a look-up request for ( Vreq  , PubGx) and sends it to
    Gh
i
 2: Gh broadcasts the request; every group head $G_j$ receiving the broadcast
    message follows these steps:
 3: if Gh finds  Vreq   its Resource type then
 4:     if Gh has  Vreq   then
 5:         Gh encrypts $E(Vdata, PubGx)$ and sends it back to Gx using
            the same path it received  Vreq
 6:         Gx, after receiving, decrypts $D(E(Vdata, PubGx), PvtGx)$
 7:     else
 8:         Gh broadcasts in its group $G\_j$
 9:         if Group $G\_y$ has  Vreq   then
10:             Gy encrypts $E(Vdata, PubGx)$ and sends it back to Gx
                using the same path it received  Vreq
11:             Gx, after receiving, decrypts $D(E(Vdata, PubGx), PvtGx)$
12:         end if
13:     end if
14: end if
```

To generate proof and build confidence in ZKP maintenance protocol, the starting group head or the prover suggests a one-step challenge Puzreq, such as computing the SHA-256 hash of a random number. This random number can be altered to introduce a new challenge at each step and create a new reandom number. Upon receiving the Puzreq, the verifiers will devise a puzzle and forward it to the prover, setting a timeout period of T Pout. In case the prover respond within T Pout, the verifiers will check the response from the prover. If the response is incorrect, they will send the puzzle back to the prover, allowing them another opportunity to demonstrate their trust. The number of attempts can be set by the network administrator. The number of attempts can be set by the network administrator. If the response does not arrive within T Pout, the verifier will send the puzzle back to the prover, offering them another opportunity to prove their trust. Similarly, the number of attempts can be set by the network administrator. This process is essential because there's a possibility that the prover is trustworthy, but due to network delays, the response does not arrive within the specified T Pout. The scenarios are represented in figures 3, 6, and 7.

Whenever the ZKP maintenance protocol is started by the group head, for instance, Gh, the verifiers will record the time of its initiation. If it take longer than a predetermined time frame (established by the network administrator) after the initial recording, the verifiers will flag this as suspicious activity and increment the trust factor for that particular group head in the IRT. They will then notify all group heads of the updated IRT, prompting them to update their own IRT. This procedure guarantees continuous maintenance in the RC-based network and maintains trust among the group heads.

and maintains trust among the group heads. Let us consider a RC-based network with 10 resource types, therefore, the group numbers range from (G h 0 ..... G h 9), the group head of group 0, G h 0 wants to initiate the ZKP maintenance protocol, then G h 0 is the Prover and G h 1 , G h 9 and G sh 2 0 will be the Verifier. The ZKP maintenance protocol initiated by every group head is given in algorithm 1.

3.1 Secured Data Look-up and transfer Protocol for RCbased P2P netwo

Through the use of ZKP maintenance protocol proposed in algorithm 1, we can assure that there is trust being developed between the group-heads, as the group heads being the center of target for the network. The Trust Factor (TF) is specifically designed to make the protocol tolerant and give opportunity to the group-heads to prove their trust. Given this scenario, we propose the following data transfer protocol which happens after a successful data-lookup being done using the protocols proposed by the authors in [33]. Let us consider that peer G x i Gi is querying for a resource ¡ Vreq ¿. The broadcast protocol is used as described in [20]. The secured data-transfer protocol is presented in algorithm 2.

4 Evaluation

Our protocols, ZKP maintenance protocol and the secured data look-up and transfer protocol proposed in section 3 was thoroughly assessed, taking into account various conditions. The proposed data-lookup protocol unlike in [11], requires less number of hops to transfer the secured content from the destination to the source. The reason being in [11], every time a data look-p is initiated, the ZKP protocol was initiated, whichadded to the number of hops required to maintain trust, look-upand transfer of data. That is the reason why we proposed onmaking our ZKP as a maintenance protocol as it will not affectthe data look-up and transfer scenarios. Every time the ZKPmaintenance protocol is initiated, it develops thetrust between the group heads present in the RC-based P2P network.

On the other hand the protocols proposed in [11] were rigid in nature, thereby not letting the peers to rectify their mistakes or in other words good behaviour was not rewarded. We have that option in our protocols, as good/trusted behaviours are rewarded. The Trust Factor (TF) is proposed to increase if a malicious behaviour is noticed, and decreased if the peer is having trustworthy behaviour.

5 Conclusions

By utilizing Zero-Knowledge Proof (ZKP) maintenance protocol, our innovative approach effectively addresses the crucial problem of building and preserving trust in peer-to-peer(P2P) networks, guaranteeing optimal security, privacy, tolerant and speed in data transfers. By managing trust verification and maintaining a balance between user anonymity and node validity, the protocol improves network security and scalability while lowering the likelihood of malicious assaults. This enhances user experiences, increases network resiliency, and facilitates smooth data flows. Trust verification is a difficult issue in RC-based P2P networks since there is no central authority to manage the nodes that join and leave the network on a regular basis. In this study, we provided a trust model intended for P2P networks based on RC. We use a confidence Factor (TF) in combination with the Zero-Knowledge Proof (ZKP) concept to establish confidence.

Our future work for this paper will be concentrated on developing the algorithms in such a way that the overheads are reduced for mobile and IoT environments due to resource constraints. We also want to further expand the concepts proposed in this paper to include dynamic trust adaptation mechanisms that will adjust the Trust Factor (TF) based on realtime network configurations, which will enhance the model's resiliency towards the ever-changing P2P environments. We plan to integrate blockchain and machine learning technologies which further strengthen the model's robustness.

Acknowledgments

1. Karl Aberer and Zoran Despotovic. Managing trust in a peer-2-peer information system. In Proceedings of the Tenth International Conference on Information and Knowledge Management, CIKM '01, page 310–317, New York, NY, USA, 2001. Association for Computing Machinery.
2. Lyes Badis, Mourad Amad, Djamil A¨ıssani, Kahina Bedjguelal, and Aldja Benkerrou. "ROUTIL: P2P Routing Protocol Based on Interest Links". In 2016 International Conference on Advanced Aspects of Software Engineering (ICAASE), IEEE, pp. 1 - 5, 2016.
3. Shane Balfe, Amit D Lakhani, and Kenneth G Paterson. Trusted computing: Providing security for peer-to-peer

networks. In Fifth IEEE International Conference on Peer-to-Peer Computing (P2P'05), pages 117–124. IEEE, 2005.

4. Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Scalable zero knowledge with no trusted setup. In Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part III 39, pages 701–732. Springer, 2019.
5. Ahmet Burak Can and Bharat Bhargava. Sort: A self- organizing trust model for peer-to-peer systems. IEEE Transactions on Dependable and Secure Computing, 10(1):14–27, 2013.
6. Yatin Chawathe, Sylvia Ratnasamy, Lee Breslau, Nick Lanham, and Scott Shenker. "Making Gnutella-like P2P Systems Scalable". In Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, SIGCOMM '03, New York, NY, USA. Association for Computing Machinery, pp. 407-418, 2003.
7. Rube´n Cuevas, Michal Kryczka, Angel Cuevas, Sebastian Kaune, Carmen Guerrero, and Reza Rejaie. Unveiling the incentives for content publishing in popular bittorrent portals. IEEE/ACM Transactions on Networking, 21(5):1421–1435, 2013.
8. E. Damiani, S. De Capitani Di Vimercati, S. Paraboschi, and P. Samarati. Managing and sharing servants' reputations in p2p systems. IEEE Transactions on Knowledge and Data Engineering, 15(4):840–854, 2003.
9. Ernesto Damiani, De Capitani di Vimercati, Stefano Paraboschi, Pierangela Samarati, and Fabio Violante. A reputation-based approach for choosing reliable resources in peer-to-peer networks. In Proceedings of the 9th ACM conference on Computer and communications security, pages 207–216, 2002.
10. George Danezis and Prateek Mittal. Sybilinfer: Detecting sybil nodes using social networks. In Ndss, pages 1–15. San Diego, CA, 2009.
11. Sai Kiran Deverasetti, Anjila Neupane, Indranil Roy, Reshmi Mitra, and Bidyut Gupta. Establishing trust using zero knowledge succinct proof in peer-to-peer data transfer. In Proceedings of 36th International Conference on, volume 97, pages 91–100, 2024.
12. Xinxin Fan, Ling Liu, Mingchu Li, and Zhiyuan Su. Grouptrust: Dependable trust management. IEEE Transactions on Parallel and Distributed Systems, 28(4):1076–1090, 2017.
13. Rzan Tarig Frahat, Muhammed Mostafa Monowar, and Seyed M Buhari. Secure and scalable trust management model for iot p2p network. In 2019 2nd International Conference on Computer Applications Information Security (ICCAIS), pages 1–6. IEEE, 2019.
14. Prasanna Ganesan, Qixiang Sun, and Hector Garcia-Molina. "Yappers: A Peer-to-Peer Lookup Service Over Arbitrary Topology". In IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428), 2: 1250–1260, 2003
15. S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. SIAM J. Comput., 18(1):186–208, feb 1989.
16. Mo Hai and Yan Tu. "A P2P E-Commerce Model Based on Interest Community". In 2010 International Conference on Management of e-Commerce and e- Government, IEEE, pp. 362-365, 2010.
17. M Harikrishnan and KV Lakshmy. Secure digital service payments using zero knowledge proof in distributed network. In 2019 5th International Conference on Advanced Computing Communication Systems (ICACCS), pages 307–312. IEEE, 2019.
18. Swathi Kaluvakuri, Bidyut Gupta, Banafsheh Rekabdar, Koushik Maddali, and Narayan Debnath. Design of rc-based low diameter two-level hierarchical structured p2p network architecture. In Mohammed Serrhini, Carla Silva, and Sultan Aljahdali, editors, Innovation in Information Systems and Technologies to Support Learning Research, pages 312–320, Cham, 2020. Springer International Publishing.
19. Swathi Kaluvakuri, Bidyut Gupta, Banafsheh Rekabdar, Koushik Maddali, and Narayan Debnath. Design of rc-based low diameter two-level hierarchical structured p2p network architecture. In Mohammed Serrhini, Carla Silva, and Sultan Aljahdali, editors, Innovation in Information Systems and Technologies to Support Learning Research, pages 312–320, Cham, 2020. Springer International Publishing.
20. Swathi Kaluvakuri, Bidyut Gupta, Banafsheh Rekabdar, Koushik Maddali, and Narayan Debnath. Design of rc-based low diameter two-level hierarchical structured p2p network architecture. In Innovation in Information Systems and Technologies to Support Learning Research, pages 312–320, Cham, 2020. Springer International Publishing.
21. Swathi Kaluvakuri, Koushik Maddali, Nick Rahimi, Bidyut Gupta, and Narayan Debnath. Generalization of rc-based low diameter hierarchical structured p2p network architecture. International Journal of Computer and Their Applications, page 74, 2020.
22. Swathi Kaluvakuri, Nick Maddali, Koushik sand Rahimi, Bidyut Gupta, and Narayan Debnath. Generalization of rc-based low diameter hierarchical structured p2p network architecture. International Journal of Computers and Their Applications, 27(2):74–83, 2020.
23. Swathi Kaluvakuri, Indranil Roy, Koushik Maddali, Bidyut Gupta, and Narayan Debnath. "Efficient Secured Data Lookup and Multicast Protocols with Anonymity in RC-Based Two-level Hierarchical Structured P2P Network.". International Journal for Computers Their Applications, 28(3):140-149, 2021.

24. Sepandar D. Kamvar, Mario T. Schlosser, and Hector Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In Proceedings of the 12th International Conference on World Wide Web, WWW '03, page 640–651, New York, NY, USA, 2003. Association for Computing Machinery.
25. Mujtaba Khambatti, Kyung Dong Ryu, and Partha Dasgupta. "Structuring Peer-to-Peer Networks Using Interest-based Communities". In International Workshop On Databases, Information Systems, and Peer-to-Peer Computing, Springer, pp. 48–63, 2003.
26. Dmitry Korzun and Andrei Gurtov. "Hierarchical Architectures in Structured Peer-to-Peer Overlay Networks". Peer-to-Peer Networking and Applications, Springer, 7(4):359-395, 2014.
27. Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In 2016 IEEE symposium on security and privacy (SP), pages 839–858. IEEE, 2016.
28. Xiaoyong Li, Feng Zhou, and Xudong Yang. Scalable feedback aggregating (sfa) overlay for large-scale p2p trust management. IEEE Transactions on Parallel and Distributed Systems, 23(10):1944–1957, 2012.
29. Li Lu, Jinsong Han, Yunhao Liu, Lei Hu, Jin-Peng Huai, Lionel Ni, and Jian Ma. Pseudo trust: Zero-knowledge authentication in anonymous p2ps. IEEE Transactions on Parallel and Distributed Systems, 19(10):1325–1337, 2008.
30. Koushik Maddali, Banafsheh Rekabdar, Swathi Kaluvakuri, and Bidyut Gupta. Efficient capacity-constrained multicast in rc-based p2p networks. In Proceedings of 32nd International Conference on, volume 63, pages 121–129, 2019.
31. Will Major, William J Buchanan, and Jawad Ahmad. An authentication protocol based on chaos and zero knowledge proof. Nonlinear Dynamics, 99:3065–3087, 2020.
32. Xianfu Meng and Dongxu Liu. Getrust: A guarantee-based trust model in chord-based p2p networks. IEEE Transactions on Dependable and Secure Computing, 15(1):54–68, 2018.
33. Anjila Neupane, Reshmi Mitra, Indranil Roy, Bidyut Gupta, and Narayan Debnath. Efficient and secured data lookup protocol using public-key and digital signature authentication in rc-based hierarchical structured p2p network. International Journal for Computers Their Applications, 30(2), 2023.
34. Lawrence Page, Sergey Brin, Rajeev Motwani, and Terry Winograd. The pagerank citation ranking: Bringing order to the web. Technical report, Stanford infolab, 1999.
35. Zhuo Peng, Zhenhua Duan, Jian-Jun Qi, Yang Cao, and Ertao Lv. "HP2P: A Hybrid Hierarchical P2P Network". In First International Conference on the Digital Society (ICDS'07), IEEE, pp. 18, 2007.
36. Claudia Daniela Pop, Marcel Antal, Tudor Cioara, Ionut Anghel, and Ioan Salomie. Blockchain and demand response: Zero-knowledge proofs for energy transactions privacy. Sensors, 20(19):5678, 2020.
37. Yingying Ren, Zhiwen Zeng, Tian Wang, Shaobo Zhang, and Guoming Zhi. A trust-based minimum cost and quality aware data collection scheme in p2p network. Peer- to-Peer Networking and Applications, 13:2300–2323, 2020.
38. Ali Aydin Selcuk, Ersin Uzun, and Mark Resat Pariente. A reputation-based trust management system for p2p networks. In IEEE International Symposium on Cluster Computing and the Grid, 2004. CCGrid 2004., pages 251–258. IEEE, 2004.
39. Kai Shuang, Peng Zhang, and Sen Su. "Comb: A Resilient and Efficient Two-hop Lookup Service for Distributed Communication System". Security and Communication Networks, 89:62-71, 2022.
40. ANTONINO SIMONE, BORIS SˇKORIC´ , and NICOLA ZANNONE. Flow-based reputation: More than just ranking. International Journal of Information Technology Decision Making, 11(03):551–578, 2012.
41. S. Song, K. Hwang, R. Zhou, and Y.-K. Kwok. Trusted p2p transactions with fuzzy reputation aggregation. IEEE Internet Computing, 9(6):24–34, 2005.
42. Xiaoqiang Sun, F Richard Yu, Peng Zhang, Zhiwei Sun, Weixin Xie, and Xiang Peng. A survey on zero-knowledge proof in blockchain. IEEE network, 35(4):198–205, 2021.
43. Patrick P Tsang and Sean W Smith. PPAA: Peer-to-peer anonymous authentication. In Applied Cryptography and Network Security: 6th International Conference, ACNS 2008, New York, NY, USA, June 3-6, 2008. Proceedings 6, pages 55–74. Springer, 2008.
44. Zhiyong Tu, Wei Jiang, and Jinyuan Jia. "Hierarchical Hybrid DVE-P2P Networking Based on Interests Clustering". In 2017 International Conference on Virtual Reality and Visualization (ICVRV), IEEE, pp. 378–381, 2017.
45. Shangguang Wang, Zibin Zheng, Zhengping Wu, Michael R. Lyu, and Fangchun Yang. Reputation measurement and malicious feedback rating prevention in web service recommendation systems. IEEE Transactions on Services Computing, 8(5):755–767, 2015.
46. Yao Wang and Julita Vassileva. Bayesian network-based trust model in peer-to-peer networks. In Proceedings of the Workshop on Deception, Fraud and Trust in Agent Societies, pages 57–68. Citeseer, 2003.
47. Li Xiong and Ling Liu. Peertrust: supporting reputation-based trust for peer-to-peer electronic communities. IEEE Transactions on Knowledge and Data Engineering, 16(7):843–857, 2004.
48. Ming Xu, Shuigeng Zhou, and Jihong Guan. "A New and Effective Hierarchical Overlay Structure for Peer-to-Peer Networks". Computer Communications, Elsevier,

34(7):862-874, 2011.

49. Min Yang and Yuanyuan Yang. ”An Efficient Hybrid Peer-to-Peer System for Distributed Data Sharing”. IEEE Transactions on computers, IEEE, 59(9):1158-1171, 2009.
50. Xiaohui Yang and Wenjie Li. A zero-knowledge-proof-based digital identity management scheme in blockchain. Computers Security, 99:102050, 2020.
51. Shanyu Zhao, Virginia Lo, and C Gauthier Dickey. Result verification and trust-based scheduling in peer-to-peer grids. In Fifth IEEE International Conference on Peer- to-Peer Computing (P2P’05), pages 31–38. IEEE, 2005.
52. Runfang Zhou and Kai Hwang. Powertrust: A robust and scalable reputation system for trusted peer- to-peer computing. IEEE Transactions on Parallel and Distributed Systems, 18(4):460–473, 2007.
53. Runfang Zhou, Kai Hwang, and Min Cai. Gossiptrust for fast reputation aggregation in peer-to-peer networks. IEEE Transactions on Knowledge and Data Engineering, 20(9):1282–1295, 2008.

Authors

Anjila Neupane (photo not available) is pursuing her masters in Applied Computer Science from Southeast Missouri State University. She have completed her Bachelors Degree in Computer Engineering from Tribhuwan University in Kathmandu, Nepal. Her primary research interests revolve around peer-to-peer (P2P) networks and their applications. She is particularly interested in exploring the potential of P2P systems to improve communication and information sharing among individuals and organizations.

Indranil Roy (photo not available) 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.

Reshmi Mitra (photo not available) is an Associate 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 RD Center. Her research interests include Security and Performance issues in IoT, Cloud Computing, and Blockchain.

Bidyut Gupta (photo not available) received his M. Tech. degree in Electronics Engineering and Ph.D. degree in Computer Science from Calcutta University, Calcutta, India. At present, he is a professor at the School of Computing (formerly Computer Science Department), Southern Illinois University, Carbondale, Illinois, USA. His current research interest includes design of architecture and communication protocols for structured peer-to-peer overlay networks, security in overlay networks, and block chain. He is a senior member of IEEE and ISCA.

Narayan Debnath (photo not available) earned a Doctor of Science (D.Sc.) degree in Computer Science and also a Doctor of Philosophy (Ph.D.) degree in Physics. Narayan C. Debnath is currently the Founding Dean of the School of Computing and Information Technology at Eastern International University, Vietnam. He is also serving as the Head of the Department of Software Engineering at Eastern International University, Vietnam. Dr. Debnath has been the Director of the International Society for Computers and their Applications (ISCA) since 2014. Formerly, Dr. Debnath served as a Full Professor of Computer Science at Winona State University, Minnesota, USA for 28 years (1989-2017). Dr. Debnath has been an active member of the ACM, IEEE Computer Society, Arab Computer Society, and a senior member of the ISCA.