A Robust and Systematic Strategy towards Extenuating Sybil Attack in a Peer-to-Peer Network.

Opuh Jude Iwedike[1]
Computer Science department, Southern Delta University Ozoro, Delta State. Nigeria. opuhji@dsust.edu.ng

OVILI Henry Peter[2]
Department of Information Systems and Technology, Southern Delta University Ozoro, Delta State. Nigeria. *ovilihap@dsust.edu.ng*

Nwachokor, Samuel Chukwuemeka[3]
Computer Science department, Southern Delta University Ozoro, Delta State. Nigeria. nwachokorsc@dsust.edu.ng

Adamugono Endurance[4]
Software Engineering department, Southern Delta University Ozoro, Delta State. Nigeria. *adamugonoe@dsust.edu.ng*

Daniel Ukpenusiowho[5]
Department of Software Engineering, Southern Delta University, Ozoro, Delta State, Nigeria.
ukpenusiowhod@dsust.edu.ng

Oshiokpu Ijeoma Edith [6]
Library and information science department, Southern Delta University Ozoro, Delta State. Nigeria. *oshiokpuei@dsust.edu.ng*

ORUGBA KENNETH OBOKPARO[7]
Department of Information Systems and Technology, Southern Delta University Ozoro, Delta State. Nigeria.
orugbako@dsust.edu.ng.

EKENO Precious Eroboghene [8]
Library and information science department, Southern Delta University Ozoro, Delta State. Nigeria. *ekenope@dsust.edu.ng*

Abstract
The systematic study of relevant measures in extenuating Sybil attack by our developed, robust and fortified peer-to-peer system is a fundamental aim in this work. This work was designed to accommodate peer registration phase, ensuring peers satisfied communicated requirement as well as request for connection to the super peer. The coordinating agent module in the network reveal any malicious peer intention to connect with peers, certifying Super Peer dominance as well as no pairing for peer communication on the network. A peer restriction policy was incorporated in this study to guarantee systematic or automatic generation of a Communication Identity Code (CIC) on confirming successful peer registration and display error for peers trying to illegitimately connect on the network. The RSA cryptosystem as well as additional security layer. SHA3-1024 were utilized in assuring a robust and fortified system. The results of this study suggest as well as communicate a robust, reliable, better improvement and developed arrangement to handle Sybil attack in Peer-to-Peer system.
Keywords: Peer-to-peer, Communication Identity Code, RSA, Secure Hash Algorithm.

1.0 Introduction

The emergence of peer-to-peer (P2P) systems, in the past years of persistent effort, have changed the approach in disseminating information as well as techniques in retrieving information from collaborating or distributed systems. This peer-to-peer system is in contrast with the well-known client-server computation arrangement. The peer-to-peer systems predominantly are known to be decentralized distributed systems having equitably different computing components called peers. Koubarakis (2003) revealed that peers co-operate in exchanging or consuming services/resources with each other in a network. Nodes in this arrangement create a partial network that are seen as

overlay network placed over a visible network, in this instance like the Internet. The topology in a peer-to-peer system signifies the manner its peers will be positioned on the partial network.

Peer-to-peer system or computing is intermittently taking by researchers to lightly define the arrangement of a distinct peer-to-peer network and both will be engaged interchangeably in this study. The inception of well-known peer-to-peer setups such as Napster and Gnutella resulted to an eruption of concern in this network arrangement together with individuals researching and practicing. Swamynathan et al (2010) said that to minimize risks and promote reliability, applications entail managing trust relationships among users in motivating cooperation and genuine participation. This change was largely linked to users cooperating anonymously with one another in these domains leading to users being subjected to risks. Chen et al (2010) mentioned that the effective realization of their intentions for anonymous cooperation makes it comparatively efficient, dependable and secure network.

Also, this kind of peer-to-peer network for clarity are known to be pure, centralized or hybrid. In pure peer-to-peer, the complete network comprises exclusively servant peers. In a centralized linked peer-to-peer system, the central server is used principally for indexing, holding track of information, incorporating every participating nodes activity and putting control on the overall system. Hybrid peer-to-peer in this context relies on incorporated features associated with pure and centralized peer-to-peer arrangement to yield certain functionalities as well as file exchange dispersed through the centralized nodes branded Sponsor nodes. Sponsor node is designed and trusted to handle high responsibility task/function in peer-to-peer system. Dasgupta, (2003) proposed that a peer-to-peer design permit mobile agents to be taken as peer acting like mediators, substituting initial message-based practices to realize enhanced efficiency, reliability and scalability.

Juan and Zheng (2012) said the motive that resulted to the desire for an improved standard shared data plan for data communication and integration among heterogeneous applications and structures are the merits of interoperability. The major causes of these attacks that makes them effective is due to the design emanating from today's Internet. The Internet is intended for speed in sending of packets and gave less attention to the challenges of security. Gancheva et al (2011) declared that the database acquired from the various scientific study were typically heterogeneous and dispersed in peer-to-peer network. According to Hutchins et al (2011), multitude of facts revealed that the Internet was not intended to monitor traffic and thus risk IP Spoofing. The design features afford multiple opportunities for diverse forms of DDoS attacks. Botnets are mostly used as the platform of interest to execute DDoS pattern of attacks owing to

distinct anonymity it offers to attacker and possessing ability to achieve high traffic volumes with negligible instructions being forwarded. It is anticipated that our research work will enhance the system against likely peculiar security attacks affecting peer-to-peer network. Danezis (2005) stated that an exciting dissimilarity is to save record trail whereby peers induct unknown peers to be part of the network. The Sybil attack usually start with a malicious node convincing a non-malicious node in admitting its request in connecting to the network. The successful connection to the network by a malicious node provide an easy entrance to persuade its other accomplices connecting straight to the network devoid of having to influence further the non-malicious node. Marques et al (2001) stated that mobile agent's distinctive characteristics and behaviours necessitate the host to recognize mechanism to be adopted in communicating with all fresh agents and their operations. Pang et al (2003) explained two concepts for secure computing using agents that are mobile in nature and peer-to-peer network. In this study, we anticipate that each peer is meant to possess private/public distinct keys required for signing, absolute encrypting and decrypting of messages.

Charu.(2012).averred that mobile agents are software program that migrates from one peer to another while performing given tasks on behalf of a user. Mobile agent recently can function asynchronously and independently. Mobile agents are programs with persistent identity that move around a network on their own volition, communicate with their environment and other agents.

William (2011) attest that plaintext is the actual data prior to being encrypted and data of encryption output is branded cipher text or cryptogram. Cryptography likewise is the study of surreptitious (crypto-) and writing (-graphy) independently. It is a framework that ensure keeping and transferring data or message safely in a specific manner such that only intended recipient can read and communicate appropriately. In latest computer technology, this cryptography is mostly linked with scrambling regular text (branded as plaintext) into cipher text, the outcome named as encryption and likewise back to plaintext, the effect termed decryption. The SHA-3 hash function application incorporates three brands namely initialization, absorbing and squeezing. Keccak is likened to sponge functions and from inception described in (Bertoni et al, 2011).

2.0 Literature Review

2.1 Security Issues on Peer–to-Peer System.

We communicate in this study that peers interact intentionally or unintentionally with new peers for the aim of accomplishing its core task in a peer-to-peer system. Jung-Tae (2005) communicated that the serious risks applicable to peer- to - peer systems have shifted attention

towards other security challenges like Confidentiality, Authentication, etc. in the peer-to-peer vicinity.

2.2 Taxonomy of Attacks on Peer-to-peer System

The diverse forms of attacks in this network can be reasonably categorized into two extensive classes namely Active and Passive attacks. Active attack is such that their ultimate goals are the node or nodes in a functioning network. Kahate (2011) declared that an active attack endeavours to modify system record or affect their functionality. Active attack can afterward be categorized into two precise types namely: Targeted and Opportunistic attack. A targeted attack is masterminded by an attacker that is nursing certain target or targets at heart while Opportunistic attacks are prompted directing at no precise node in mind on accessing the network. The intention initiating this kind of attack is to infiltrate numerous node and rely on the benefit of confirmed vulnerabilities assembled from those nodes. There are various breeds of peer-to-peer network menace categorized into certain kind of Opportunistic attack namely Worm, Zombification, Eclipse and Short Circuit attack: Worm operate as a self-directed code that proliferate across a network. Computer virus referred to as a destructive code that attacks files on a system. Worm is one form of a computer virus that can meddle with a local system and substantively proliferate to another system on the network. These worms can be strong worm or scanning worm, organized worm or overlay topological worm.

Xu et al (2012) deduced that active worm or scanning worm is one specific type of worm that randomly scrutinize IP addresses for their proliferation on the network. There are various attack form found in peer-to-peer network which can be grouped into some technique of Targeted attack. Like MiTM (Man in the Middle), DoS, DDoS etc. MiTM denote an attack whereby an attacker personates both ends of a secure communication device on a network.

Adeyinka (2008) maintained that this can result to the messages being meddled as well as delicate information can be hijacked this way in a peer-to-peer system. There are several brands of passive attack namely Cached Data menace, Sybil, Bootstrapping, Spamming, Identity Mapping, Routing Table menace, Passive Dos /DDoS menace and Content Availability Depletion. Douceur (2002) affirmed that Sybil refer to menace on singularity of identity whereby a single node meddles in the network by assembling illegitimate quantity of node identifiers and likewise emulating numerous legitimate nodes. Douceur (2002) declared that Sybil menace is a destructive agent deceiving several agents in a bid to coordinate a big proportion of the identifier space as well as cast multiple votes. This aids the attacker to take negligible size of nodes and inflict an irreparable harm to the network. The attacker on succeeding in gaining ample nodes in

that section compared to the authentic nodes, the attacker now manipulates every message that routes through the section. This menace can be channeled as an access to execute large magnitude attacks of other brands like Eclipse. Sybil menace is one brand of attacks on the peer-to-peer framework that introduces serious trouble in detecting it.

2.3 Related Work

Opuh et al (2021) studied a Secured Agent-based Model for Peer-to-Peer System. They emphasized that Information exchange that is devoid of control in the peer-to-peer communication, exposes peer to malicious activities, insecure communication loss of significant data or failure of the system. The complexity and perceived compromise in peers communicating at different levels necessitates modeling a secured agent-based model for a peer-to-peer system. This work was designed to accommodate peer registration phase that will allow peers on satisfying defined requirement, request for connection to the super peer, subsequently guaranteeing and promoting healthy system. The agent module in the network ascertains successfully connected peers on the network, certifying feedback agent goal and ready for peer communication. The result shows that peculiar security attacks from malicious and un-registered peers are systematically controlled in the peer-to-peer system.

Vijaya kumar et al (2016) worked on the efficient group key agreement Protocol for secure peer-to-peer communication. This effective framework of a shared group key administration for a peer-to-peer framework with negligible operational complexity in a vibrant safe group collaboration is a hard task. This is evidently owing to unavailability of a centralized controller. Consequently, top remote this project, a self-composed shared group key administrative framework was recommended for safe peer-to-peer collaboration. In this study, group key calculation was executed using CRT and fortified communication was effected adopting RSA algorithm. This arranged key control framework is a single round procedure whereby a managed group key is created using every client public key and were formed from their separate private keys. The substantial benefit of the assembled key control set-up applied in this study is that it minimizes the operational complexity from the peer participants. This decline in operational complexity is realized by executing single addition and multiplication computation in the process of a solitary client join and singular subtraction operation if a solitary member leaves. This proposed algorithm was applied and scrutinized with well-known predominant shared group key control protocols and the consequence reveal that it minimizes the operational complexity significantly.

Consequently, a fresh and effectual solution to confront the operational complexity without raising ample storage complexity in bringing safe group collaboration in this concepts and was attained through active group key management arrangement. This proposed algorithm concentrates majorly on the lessening of operational complexity in key quantifying time of client. In contemplation of the storing complexity, the quantity of keys to be kept by the group participants is marginally raised in evaluation with known peer-to-peer key controlled protocols. Substantively, the algorithm in their study necessitates each participant to transmit one broadcast message to acquaint partakers in the group concerning their public key. This message is dispatched to aid in calculating the group key and substantially sustain likewise communication complexity in both the join with leave exercise.

Xiao-Long et al (2016) worked on hybrid collaborative management ring on mobile multi-agent for cloud-peer-to-peer. They stated that in order to fully utilize all the available potential network resources, it is imperative to incorporate cloud computing and peer-to-peer computing environments. Substantially, their study utilized the mobile multi-agent technology to construct an effective hierarchical integration model named cloud peer-to-peer. Substantively, after in-depth analyses and experiment, the hybrid collaborative management ring based on mobile multi-agent depict a significant improvement. Kasyful (2017) researched on collaborative file sharing system using Jxta peer-to-peer networking infrastructure. Substantively, their work aimed to develop a simple workflow based collaborative application will be running over peer-to-peer network. Consequently, basic features of the application were to support communication, coordination in a workflow-based document production, offer services for text chat and file sharing.

Finally, they averred that the system still need to be optimized, both in software and network.

Substantively, the algorithm in their study necessitates each participant to transmit one broadcast message to acquaint partakers in the group concerning their public key. This message is dispatched to aid in calculating the group key and substantially sustain likewise communication complexity in both the join with leave exercise. Rajesh et al (2016) worked on a survey of peer-to-peer networks.

In their work, they mentioned that peer-to-peer networks have been successful in the file sharing networks (such as Napster, Gnutella, Kazaa, BitTorrent, JXTA and Freenet). More so, increase in the popularity of peer-to-peer networks has been witnessed by millions of internet users. In this study, they analyzed some network architectures evolution such as client servers, peer- to-

peer network etc, subsequently, a failure experienced by a super-peer, will not disrupt system activities in peer-to-peer network as strategies in place to take the job of the primary super-peer. Finally, they averred in their result that peer-to-peer network are steadily improving, devoid of single point of failure that has been a major issue with client server network.

Riccardo (2016) researched on a trust and reputation method to mitigate a Sybil attack in Kademlia

They communicated that peer-to-peer architectures have developed into a well-known system in the last years for ample services as well as applications such as collaborative computing, streaming and VoIP applications. The security and integrity of the overlay involved in such networks is a significant prerequisite for deploying such a technology. Also, their solution presented a balanced incorporation of standard Kademlia algorithms and trust-based algorithms showing promising results in thwarting a Sybil attack in a Kademlia network when compared with likened techniques from other studies.

2.4 Peer Restriction Policy

This entail a policy or strategy that systematically generate communication identity code for successfully approved peer first and only acceptable connection request as well as restricting illegitimate peers from connecting to the system. It enforces a one and only connection request from an intended peer to its super peer on desiring to dispatch content, interchange information or incorporate with a providing peer anticipated instruction Predominantly, once the communication identity code of the authorized provider peer is systematically generated, a surreptitious/malicious peer request restriction policy will be activated, permitting just the two paired peers to interact until the feedback agent module certifies communication successful or flop.

3.0 Materials and Methods

The sequence diagram of this study was depicted in figure1 It communicated the interaction of multiple modules regarding peer enrollment, querying, security policy, peer communication identification etc. It essentially ascertain sequence of applicable processes running on the system. The peer-to-peer communication incorporates enrollment, successive connecting and disconnecting from multiple peers in a lively network for systematic service.

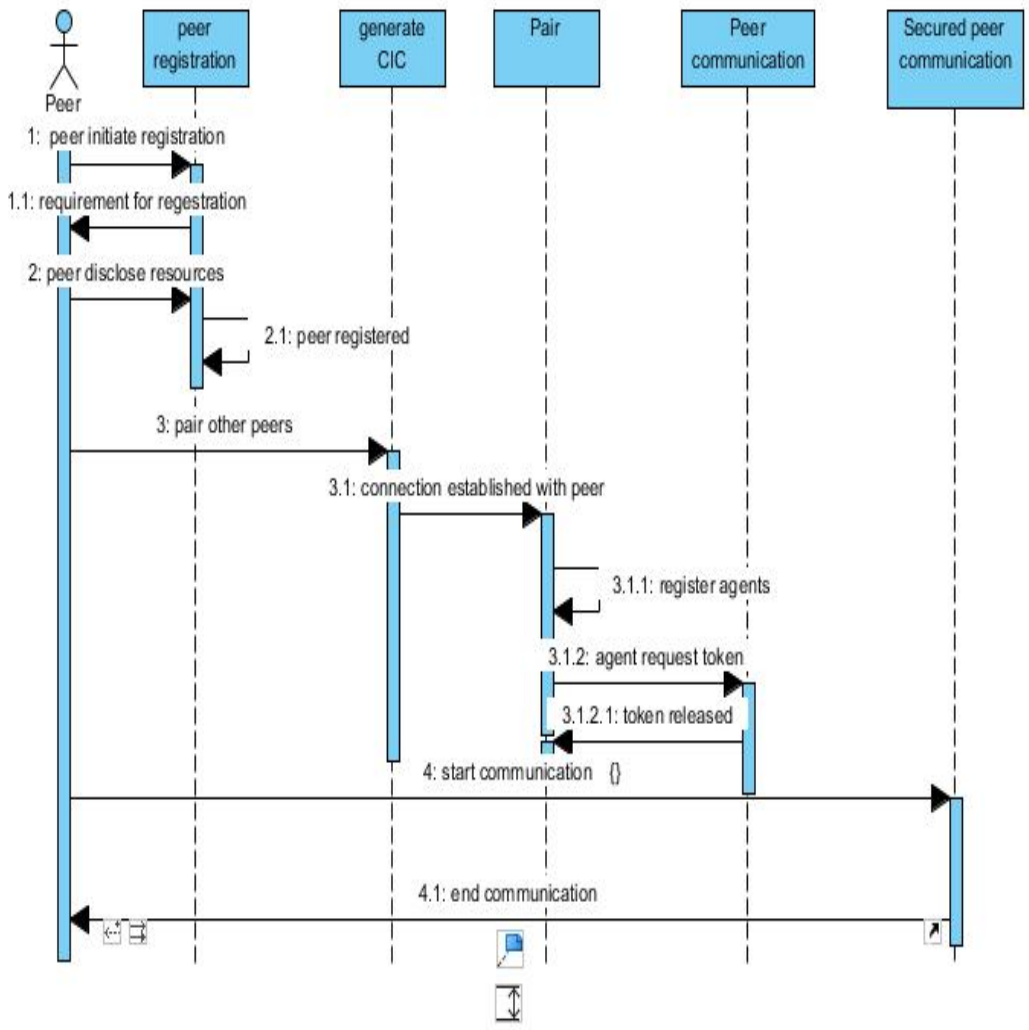


Fig1: System Sequence Diagram

3.1 Robust and Fortified SHA-3 Algorithm

Step 1 Input parameter {message type,name}

SHA3: = proc (message: : string, messagetype: : name : = text)

Step 2 Localize variable name, message, length, Local n, m, l;

Step 2.1 Continue Process

If type (procname, 'indexed ') then

Step 2.2 output length in bits with value 512, n = op (procname)

Step 3 Report error

else

error "output length not specified"

end if;

Step3.1 Output length not in conformity with specified value

if not n in (512) then

error "% 1 is not a valid output length ". n

end if "

m: = messagetobytes (message, messagetype);

Step 3.2 Generated capacity likened twice output length

l: = keccak (m, 1600, 1600 – 2. n, n, hash):

bytestohexstring (l)

Step 4 Terminate process

End proc:

3. 2 Initialization, Absorbing and Squeezing State

KECCAK is likened to sponge functions and from origin described in (Bertoni et al, 2011). The padding tenet in KECCAK is branded as multi-rate padding These KECCAK-p permutations are specified with two parameter ascertained as fixed-length strings arranged and branded the permutation width and lastly the amount of repetitions from an internal transformation attested as round. The width is symbolized as b and amount of rounds tagged as nr.

The KECCAK-p permutation having nr rounds with width b is described as KECCAK-p [b, nr]; this arrangement is substantiated for respective b of the form {25, 50….1600} devoid of negative integer nr. A process in KECCAK-p arrangement, signified by Rnd, incorporates series of 5 transformations tagged as step mappings. The permutation is specified in form of value display for b bits consistently updated, branded as the state and this state is the foremost set of feedback values in the permutation.

The acceptable way of effecting Keccak ascertained round of 24 as it relates to initialization, absorbing, squeezing and successive round of this Keccak algorithm is realized at 24. It is substantial for the Keccak's five states to be consistently executed in 24 times. In the first instance, this five states of Keccak concept are implemented, substantively it is kept as state 1 and likened to the first state and subsequent repetition of another 23statesis effected and the coding strategy is arranged in a manner that conform to intended concept in the algorithm. All these 24 states are effected one succeeding another in a consistent manner and actualizing a process will systematically act as input to the fresh succeeding state. These process succeeds all through the next 23 states and likewise output of the final 24 states gives rise to SHA-3 code.

Predominantly, the rest of this processing is affiliated to this coded output. This is acknowledged as the earliest method of affecting the Keccak algorithm that incorporates successive states reiteration.

4.0 Experiment and Results

In our previously discussed chapter, the analysis and design utilized in the problem likened to secured peer-to-peer system was substantially examined, effectual and reliable approach in alleviating security challenges in peer-to-peer concept. The agent concept in developing a secured peer-to-peer system was modeled as depicted in fig. 3., the implementation process for a secured peer-to-peer arrangement were addressed and effect generated. The effect generated, from the real world security domain of peer-to-peer communication portrayed improved security, guaranteed better peer user incorporation, justifiable plan that delights users interest in peer-to-peer system. Lastly, in this study, an effectual, reliable and robust peer-to-peer system is actualized utilizing this setup.

4.1 Peer Registration Phase

In this enrollment phase, the super peer run function, permit starting of super peer and likewise generates its IP address. The ordinary peer concept initially displayed disconnected status, likewise the SHA3 additional security were loaded on different systems, similarly generating respective peer IP addresses on connecting to the super peer with port identity and displaying connected status. These are depicted in figures 2, 3. The absolute idea in this peer enrollment phase is to ascertain the peers that will be connected to the network as well as extenuating malicious/unauthorized access/controlling of the peer-to-peer system.

4.2 Secured Peer Communication Phase

In the secured peer communication phase, it is envisaged that the incorporating peers have been successfully enrolled with their IP address and its likened generated communication identity code, pair to establish connection with each other and set for a potential communication in our peer-to-peer system. This study provided additional security for the peer-to-peer communication as illustrated in figure 4. The whole idea is to extend RSA with SHA3-512. This require ticking the button that displayed use additional security during peer-to-peer communication.

Fig 2: Super Peer Displaying Connected Status

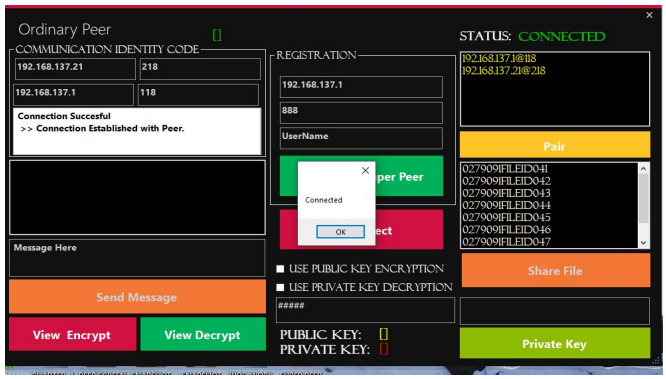


Fig 3 : Peer Displaying Pair Connect (CIC 218)

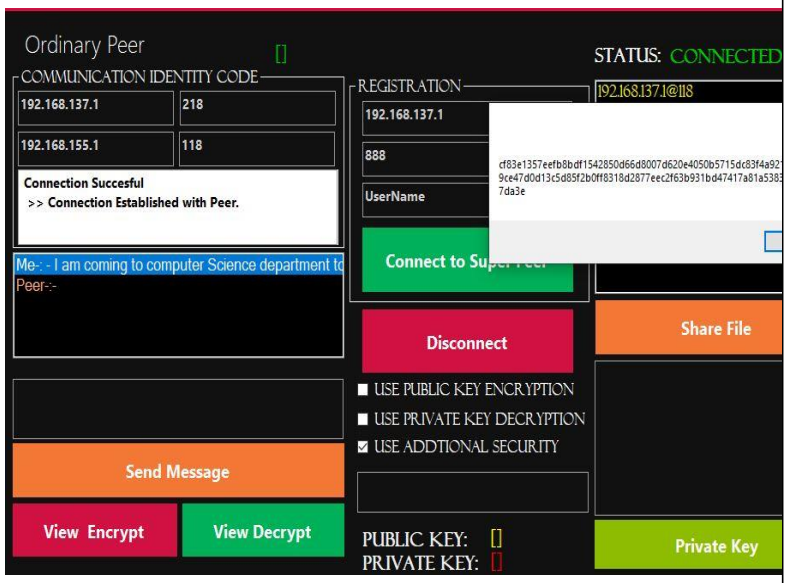


Fig 4: Peer communication generated hash message equivalent.

4.3 Results Discussion

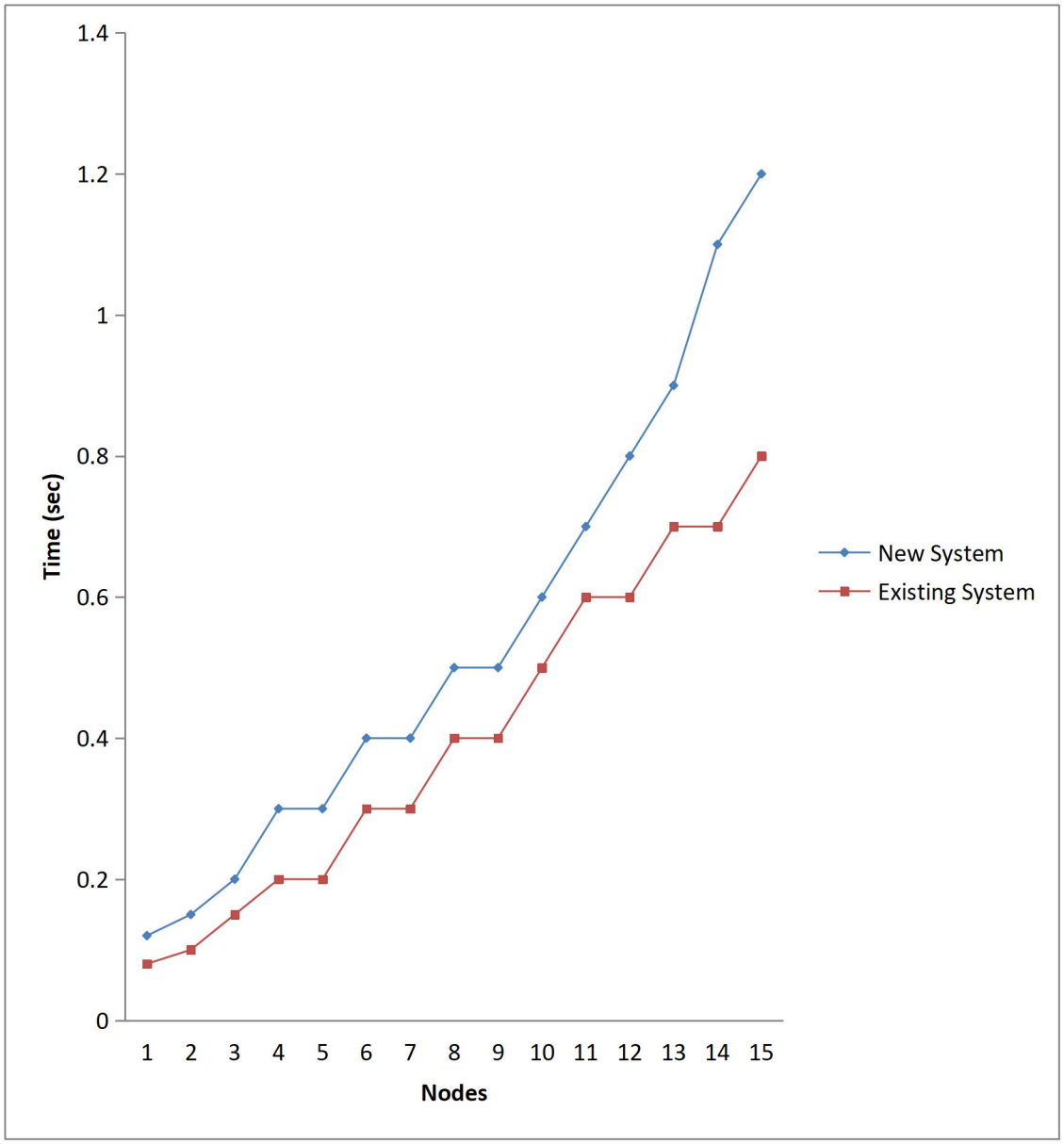
The effect of our practical description on secured encrypted/decrypted message and share file in various tables communicated earlier in this work. We executed different peer-to-peer communication to ascertain if our intention is right and the effect revealed that only peers intended to communicate send, receive messages or shared files utilizing applicable button in the system. The figures in the table were multiple effects portrayed in the course of testing our system workability. We attached some of the test executed to ascertain our findings. The result obtained as displayed assured outcomes from preimage resistance, fortified second preimage resistance.

Table 1 depicts that the extended security of peer communication as the system output hash equivalent of messages. This study graph connectivity node discovery as compared to that of the existing system was depicted in figure 5.

Table 1: Outcome of Extended Security in Secured Peer Communication

Peer Types	IP Addresses	CIC	Port ID	Status	Peer Pair Connection With CIC	Secured Encrypted/ Decrypted Message	Secured Encrypted/Decrypted shared	Extended Security of Secured Peer Communication
Super Peer	192.168.137.1		888	Connected				
Peer 1	192.168.137.1	@118	888	Connected	Established	Encrypted/Decrypted	Encrypted/Decrypted	System output Hash equivalent of message
Peer 2	192.168.137.21	@218	888	Connected	Established	Encrypted/Decrypted	Encrypted/Decrypted	System output hash equivalent of message
Peer 3	192.168.137.62	@318	888	Connected	Established	Encrypted/Decrypted	Encrypted/Decrypted	System output hash equivalent of message
Peer 4	192.168.137.71	@418	888	Connected	Established -+*9d	Encrypted/Decrypted	Encrypted/Decrypted	System output hash equivalent of message
Peer 5	192.168.137.140	@518	888	Connected	Established	Encrypted/Decrypted	Encrypted/Decrypted	System output hash equivalent of message
Peer 6	192.168.137.142	@618	888	Connected	Established	Encrypted/Decrypted	Encrypted/Decrypted	System output hash equivalent of message
Peer 7	192.168.137.165	@718	888	Connected	Established	Encrypted/Decrypted	Encrypted/Decrypted	System output hash equivalent of message
Peer 8	192.168.137.174	@818	888	Connected	Established	Encrypted/Decrypted	Encrypted/Decrypted	System output hash equivalent of message
Peer 9	192.168.155.1	@918	888	Connected	Established	Encrypted/Decrypted	Encrypted/Decrypted	System output hash equivalent of message

Fig 5: Graph of connectivity/node discovery in the new system compared with the existing system



5.0 Conclusion

In this study, we tried to understand peer-to-peer network as well as the security challenges posed by Sybil menace in such system. We delved into Sybil attack pattern in such decentralized as well as unstructured system. The CIC strategic technique was utilized in extenuating numerous illegitimate identities connecting to the network. Our study incorporated SHA3 as additional security layer that proved to be infeasible for any adversary with malicious intention connecting to the network. Lastly, this system is robust and suggest a fortified arrangement in surmounting Sybil menace in peer-to-peer network.

References

1) Adeyinka,O.(2008). Internet Attack Methods and Internet Security Technology, Modeling and Simulation, AICMS .77-82, 13-15
2) Bertoni .G, J. Daemen, M. Peeters and G. Van Assche (2011). The KECCAK reference, Version 3.0, http://keccak.noekeon.org/Keccak-reference-3.0.
3) Charu V. (2012). A Comparison of Communication Protocols for Mobile Agents, International Journal of Advancements in Technology, 3. (2.).
4) Chen,J., H.Lu and S.Bruda (2010). A reputation-based approach for countering vulnerabilities in p2p networks, in: 2nd International Conference on E-Business and Information System Security, EBISS, 263 – 266.
5) Danezis, G., C. Lesniewski-Laas, M. Kaashoek and R. Anderson.(2005) . Sybil-resistant DH routing, in Proc. 10th European Symposium on Research in Comp. Sec.305–318.
6) Dasgupta, P. (2003). Improving Peer-to-Peer Resource Discovery Using Mobile Agent Based Referrals, Proceedings of the 2nd Workshop on Agent Enabled P2P Computing,. 41-54,
7) Douceur, J. (2002). The Sybil attack, in Proc. 1st Int. Workshop on Peerto-peer Sys. IPTPS, 251–260.
8) Gancheva, V., B. Shishedjiev and E.Kalcheva-Yovkova (2011). An approach to convert scientific data description, Intelligent Data Acquisition and Advanced Computing Systems, IEEE 6th International Conference, 15-17, 564-568,
9) Hutchins,E.M., M.J. Cloppert and R.M. Amin(2011) .Intelligence -Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, in Proceeding of the 6th International Conference on Information Warfare and Security.
10) Juan, D and Q. Zheng (2012). The research on the XML-based information exchange under heterogeneous Environment in HR Outsourcing enterprises, Computer Science and Education, 7th International Conference, 14-17, .462-465.
11) Jung-Tae, K., P .Hae-Kyeong and P. Eui-Hyun (2003-2005), Security Issues in Peer-to-Peer Systems Electronics &Telecommunications Research Institute.
12) Kasyful. A (2017). Collaborative File Sharing System Using Jxta P2p Networking Infrastructure –AnApplication Development, Journal of Environmental Engineering & Sustainable Technology, 4 (1), 31-40.
13) Koubarakis, M. (2003). MultiAgent Systems and PeertoPeer Computing: Methods, Systems, and Challenges. Proc. CIA, Springer LNCS 2782. 46-61.
14) Marques, P., P. Simões., L. Silva, F. Boavida. And J. Silva (2001). Providing applications with mobile agent technology, Open Architectures and Network Programming Proceedings: 129 -136.
15) Opuh, J., Eke, B. & Williams, E.(2021). A Secured Agent-based Model for a Peer-to-Peer System, Computer Engineering and Intelligent System,, IISTE,12(2) 2222-2863.
16) Pang, X., B. Catania and K. Tan (2003). Securing your data in agent-based P2P systems. In Eighth International Conference
17) Rajesh.K, P.Suman and K.Vinod (2016). A Survey of Peer-to-Peer Networks, International Journal ofAdvanced Research in Computer and Communication Engineering.5, (4).
18) Riccardo, P. (2016). S-Kademlia: A trust and reputation method to mitigate a Sybil attack in Kademlia . Computer Networks, 94, 205-218.

19) Swamynathan, .G. K. Almeroth and B. Zhao (2010). The design of a reliable reputation system, Electronic Commerce Research 10 (4) 239 –70.
20) Vijayakumar, P., R. Naresh, D.Lazarus and I.Hafizul (2016).An efficient group key agreement protocol for secure P2P communication, Security and Communication Networks; 9:3952–3965.
21) William.S(2014). Computer Security, Third Edition http://williamstallings.com/ComputerSecurity
22) Xiao-Long.X , B. Nik and P.Norrington(2016). Hybrid Collaborative Management Ring on Mobile Multi-agent for Cloud-P2P, International Journal of Automation and Computing 13(6), 541-551.
23) Xu.Y, C. Deng and M. Gao (2012).The Topology of P2P Network, Journal of emerging trends in computing and information sciences. 3, 8, 2079-8407.