Improved Cryptographic Algorithm for Secured Peer-to-Peer Communication System

Jude I. Opuh
Department of Computer Science
University of Port Harcourt,
Rivers State, Nigeria

Bartholomew O. Eke
Department of Computer Science
University of Port Harcourt,
Rivers State, Nigeria

Edem E. Williams
Department of Computer Science
University of Calabar,
Cross Rivers State,
Nigeria

ABSTRACT
This study entails pairing peers that indicated interest to communicate in the peer-to-peer system. Subssequently, a peer restricter policy was introduced to ensure systematic and automatic generation of a Communication Identity Code (CIC) for every successfully registered peer and any deviation to manipulate the system display error. This CIC ensure first and only acceptable connection request to a distinct authorized registered peer in the network. The communication identity code guarantees authentication of communicating peers at both end thus displaying a connection established with peer, assuring non-repudiation by the paired peers. The last phase requires activation ,incorporation of diverse agent functionalities that facilitates message exchange of peers and it is imperative to secure every communication from an un-intended recipient peer in this peer-to-peer system using RSA cryptosystem as another security layer.SHA3-1024 *was used in extending RSA* as it provided added capability in *securing the system.* The displayed encrypted and decrypted feedback messages assured security, fulfils proactive and goal directed features of agent in this peer-to-peer system.

Keywords
Peer-to-peer, Communication Identity Code, Secure Hash Algorithm, Encryption and Decryption

1. INTRODUCTION
In this paper, peer-to-peer systems fundamentally are known to be decentralized distributed systems having equitably diverse computing components called peers. These peers in actual sense are joined to few or additional more peers found or already present in the network. Peer-to-peer network are dynamic and demands steady availability of its network thus require the presence of a specialized peer (or abundant of these peers) to monitor, hold and keep record of event on the network.

[1] posit that thereafter, researchers all over the world installed peer-to-peer network in several different applications that include Communication Application like IM (Instant Messaging), Distributed Computation Project like Seti@Home, gnome@home, Distributed Database System, Content Distribution System for distributing mainly digital media. Owing to the enormous attention of researchers and the strong participation of multitude of people, numerous peer-to-peer networks such like Gnutella, Pastry are patronized. [2] declared that peer-to-peer is a computing paradigm which enable the interchange of information accompanied with services openly between suppliers and the consumers for accomplishment of meaningful results. However, in reality most peer-to-peer networks are susceptible to DOS attacks owing to the homogeneity of its network resulting in higher inter-dependence among hosts.

[3] 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) separately. 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: initialization, absorbing and lastly squeezing.KECCAK is likened to sponge functions and from origin described in [4].The long problem of insecure communication among peers in a peer-to-peer system, substantially formed our statement of the problem in this paper.

2. LITERATURE REVIEW
[5] worked on the Implementation of Secure *Key Issuing Scheme*for Communication in peer-to-peer Networks. Key issuing scheme depend on the confidentiality upheld adopting surreptitious key for dissemination of information in peer-to-peer framework. IBC was conceived in peer-to-peer networks lately for the intent of identity substantiation and authentication. It was appropriate to know that the fresh IBC-based solutions were not handling the consequences in secure private key-issuing. The work introduces a new protected key issuing set-up provided in peer-to-peer networks with IBC. It afforded IBC framework, setup phase adopting peer registration explanation through Shamir's (k, n) hidden distributing scheme, a safe key issuing structure that depend on KGC with KPAs to generate and apportion private keys to peers safely. This makes IBC systems suitable and appropriate in our today's world peer-to-peer concepts. The progressing networks demanded a requirement of resilient security and this attribute of networks likened security was satisfactorily handled. There were diverse ways to powerfully tackle the security necessity in peer-to-peer framework.

Peer-to-peer concepts has played a magnificent role in today's swift evolving world and seem very substantial to manage it competently. Security of these framework can be handled on numerous levels of cryptographic abstractions and such levels were explored with particular degree of threshold attitude. Consequently, their work concentrated on key exchanging level of a cryptographic concept and the keys are handled by the authenticated nodes partaking in the communication.

Furthermore, the research substantially applied a fresh safe key issuing set-up that utilizes basic cryptographic qualities like encryption or decryption. This absolutely concentrated on key issuing portion of cryptography as previously proposed strategy did not tackle the issue appropriately. For instance, PKI were utilized for key issuing even though it has inadequacy of handling certificates owing to the burdensome nature of these certificates in the public-key infrastructure. This constraint necessitates the request for IBC that was of enhanced efficiency equated to public-key infrastructure.

Lastly, this research work accomplished a protective key issuing arrangement in peer-to-peer framework applying IBC and developed a peer registration service adopting Shamir's surreptitious sharing algorithm. They produced a safe key issuing procedure that utilizes KGC and KPAs to assign private keys to peers safely and can overpower Sybil attacks with support of the byzantine fault tolerance.

[6] researched 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, to promote 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.
[7] researched on designing a Super peer network. Their study signifies that a super- peer is a node found in the peer-to-peer framework, operating like a server to classes of clients and likewise equivalent in the set-up of super-peers. Super peer networks incorporate stability concerning the proficiency of consolidated search, autonomy, load stability and strength to menace emanating from shared search. Substantively, it takes brilliance in the diversity of competence (for instance Bandwidth, strength in processing) regarding peers as latest research have depicted to be massive. Substantially, the fresh and ancient peer-to-peer concepts, for instance KaZaA amd likewise Gnutella were effecting super-peers as instrumental to their design. This study examined super-peer concept to a greater extent, gathered knowledge of their indispensable uniqueness and performance capabilities. Super peer schemes are effectual essentially owing to their ability in incorporating the effectiveness of the fused client-server concept possessing autonomy, load stability and strength in distributed search. It also takes brilliance in heterogeneity properties regarding peers and well-arranged super peer networks assure better performance boost for the peer-to-peer set-up. It is substantial to base design consequence on a solid conception of the system's conduct instead of speculation presently being used. This work resolved this need by presenting a scientific foundation and appreciable studying of the super-peer arranged performance. In certainty, they took consciousness of redundancy in the super-peer arrangement, topology disparities and prudently appraised super-peer network performance. Finally, the findings were able to substantiate vital tradeoffs, a universal design pattern, local decision taking positions to adaptively and systematically actualize a universally proficient system.

[8]worked on the Anonymous communication in peer-to-peer networks for providing more privacy and security. Anonymity is a relevant concern in the peer-to-peer framework. The key anonymity in peer-to-peer clients focuses on the user's disclosure and actions that may be revealed by any other user. There are ample studies recommended to provide this anonymous peer-to-peer collaboration. The recommended Dual-Path peer-to-peer nameless algorithm guarantees a rigidless layer for the requester to pick dual-path in linking the provider. This algorithm assures more reliability and safety against traffic scrutiny and TTL menace. Also it amplifies its fault strength as the connection between the requester and supplier is self-sufficient with transitional peers and if single intermediate peer witnesses failure, the requester can vary the dual-path to persist in its connectivity.

[9] researched on authenticationtechniques in computernetworks, They mentioned that the Internet has emerged as one of the most convenient and widely used media for exchanging information.The Internet today is faced with many challenges and one of it is to provide security. Subsequently, pursuing authentication through applicable mechanisms is a complex issue and their result provided some techniques in ameliorating security challenges.

[10] worked on enhancing reliability in peer-to-peer networks using social capital principles. They said that online file sharing is a common, important day to day activity which is on the increase with proliferation in social media , given a reliable and trusted network However, their main interest in this study, resulted in improving the existing system that maintain reliability mainly in the peer to peer file sharing paradigms.

[11] researched on collaborative file sharing system using Jxta peer-to-peer networking infrastructure . Substansively, 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

[12] researched on efficient and distributed network model for peer-to-peer systems, In this study, peer-to-peer networks are networks composed of heterogeneous and autonomous peers that cooperate with each other in a decentralized manner. All participating peers are both users , providers of resources and can access each other directly without intermediary agents. Substantially, their work introduced a self-organizing trust model (SORT) that aims to decrease malicious activity in a peer-to-peer system by establishing trust relations among peers in their proximity. Finally, their result revealed that SORT can be adapted in various peer-to-peer applications

[13] worked on a Survey and Comparison of peer-to-peer overlay network schemes They found out that over the Internet today, computing and communication environment are significantly more complex and chaotic than classical distributed systems, lacking any centralized orga-nization or hierarchical control. Consequently, their assertion was that inorder to move forward, the development community must understand the applicability of various schemes for structured and unstructured peer-to-peer network models.

[14] worked on mobile agent, a comparison review. Their study stated that mobile agent is a software program that migrates from one node to another while performinggiven tasks on behalf of a user . Mobile agent is widely used in distributed systems , can communicate with other mobile agents, stop its execution at any time, communicate with another host and resume its execution at any time been a state-full agent. Consequently, they asserted that mobile agents can be effectively used in gathering, filtering, sharing, monitoring, recommending, comparing and guiding information Pasupuleti and Mahendra.(2016) researched on High Speed Architecture for KECCACK secure hash function, Cryptography is a technique that protects the information in transit or stored from unauthorized orunexpected exposure. Their study provided security within the scope of research interest.

[15] worked on performance comparison of Keccak, Skein, Grøstl, Blake and JH: SHA-3 ,final round candidate algorithms. Their study took cognizance of various attacks on MDx family of Hash function including SHA-0 and SHA-1. National Institute of Standards and Technology scheduled a competition to augment or replace the current Hash standard SHA-2 Their result revealed that Grøstl and JH were not a good choice for security while Skein is a good option to use for long messages.

[16] worked on a survey of peer-to-peer networks .In this work, they mentioned that peer-to-peer networks have been successful in the file sharing in the 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. Finaaly, 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 clien server network.

[17] studiedthe topology of peer-to-peer network, They mentioned that peer-to-peer network is a logical overlay network built on the application of software based IP network. The topology of peer-to-peer network refers to the physical or logical interconnection between computing units in a distributed system, The kind of structure allows the client in thenetwork to share some computer resources .Finally, their result assured effectual communication in a peer-to-peer network

3. MATERIALS AND METHOD

The proposed system is depicted in fig 1. The proposed system embraced security in designing a hybrid peer-to-peer set-up incorporating agent concept and proficiently tracked through respective IP addresses for file or significant content sharing, request initialization and feedbacks. content sharing, request initialization and feedbacks. Indexing is one substantive tool relevant in the retrieval of facts as peer-to-peer search events that produce enormous traffic and super-peers are intended to provide proficient directories in peer request and potential services. Super peer network has a set of peers branded as clients and linked to a group of clients .

Peers are connected merely to a single super-peer and likewise this super-peer with its peers are branded as a cluster. *Super-peer* entailsa node which symbolizes a consolidated server for a subgroup of clients. Peers in the cluster incorporate and deliver request to their super-peer hoping to get feedback message through it or respective participating peers.

This system was additionally secured by extending RSA with SHA3-512 (Secure Hash Algorithm) and some of the concepts embraced in designing the system encompasses:

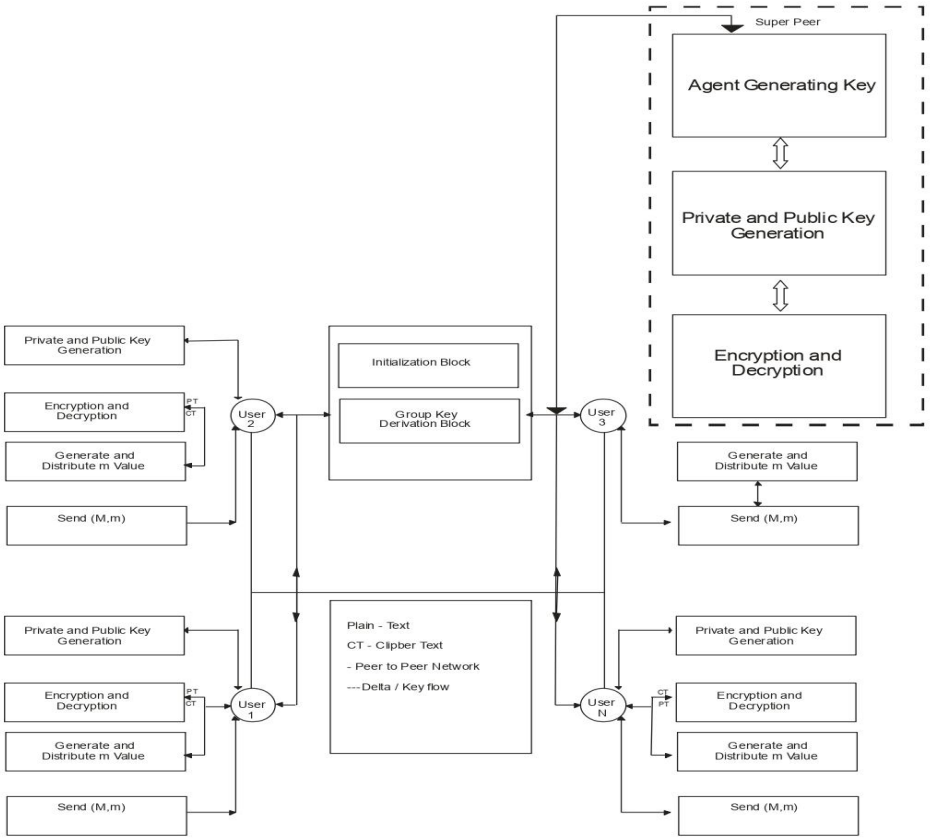

Fig 1: The Proposed System Architecture

i. Algorithm of the RSA Public-Key

Step one. Assume ekek-1 . . .e1e0, whereby, ei where i= k, k-1, k-2 to 0 as the binary
depiction e.

Step two. Set the inconstant C to be 1.

Step three. Reiterate steps three (a) and three (b) putting i = k; k-1, . . ., 0:

Step three (a) Set inconstant C into the balance of inconstant C2 while divided using n.

Step three (b). Taking ei = 1 and set inconstant C to the balance of inconstant C. M is then divided using n.

Step four. End. Precisely, C represent encrypted version of M.

This diagram in figure 3.6 depict the key pair (KRp1 as the private key of Peer1 and KUp1 is public key for Peer1) in the message exchange from sender Peer1 to the demanding Peer2 that procures and utilizes Peer1 KUp1 public- key to decrypt the message dispatched by Peer1 in the crypto arrangement.

[18]posit that an algorithm is devoted for encryption and subsequent decryption.

It is understandable that this scheme is devoid of providing confidentiality owing to everyone having access to Peer1 public key existing in public domain. Subsequently, the scheme is ineffectual since Peer2 must preserve /store likewise the message (as symbol of authenticity) and the translated plaintext (for experimental utilization of the document). An improved way of accomplishing similar result is by encrypting a fewbits *blocks* been a function to the document. This block branded as an authenticator (or symbol of authenticity), assuredly possessing the property of unfeasibility to alter the message devoid of modifying the authenticator. Subsequently, encrypting an authenticator with the message initiator private key that functions as a signature that substantiate the foundation, content and handling of the document. The scheme can be simplified as:

$Y = E_{KRp1}(X)$ ---------- 3.3

Y is an outcome ecrypting X using Peer1 private key whereby

$Z = E_{KUp2}[\ E_{KRp1}(X)]$ or $E_{KUp2}[Y]$ ---------3.4

Z is the formation of the function from this document as a symbol of authenticity whereby

$$Y = D_{KRp2}(Z) \text{ ----------3.5}$$

Y is reproduced by decrypting the message function Z for confidentiality and lastly

$X = D_{KUp1}[D_{KRp2}(Z)]$ or $DKUp_1[Y]$ ---------3.6

This scheme guaranteed secrecy, effectual authentication and was intended to display additional process of peer-to-peer incorporated, consistent and secured system.

These necessities resulted to the trapdoor single-way function been a function that links a domain into series such that a function value has special inverse, with the circumstance that the calculation of the function was streamlined and precise, though the calculation of this inverse is impossible, therefore:

$$Y = f(X) \text{ is simple}$$

(It is simple attesting that it can be calculated in polynomial time as an application of input length n where time is proportional to n^a and a is a fixed constant)

$X = f^{-1}(Y)$ is impracticable

(Impraticable necessitates that it cannot be calculated in polynomial time as an application of input length where time is proportional to 2^n)

ii. Private Key

Private Key are utilized in peer-to-peer concept to decrypt messages encoded with a likened public key. Private keys are expected to be kept surreptitious by respective enrolled peers for effectual and reliable peer-to-peer incorporation. Private key is intended not to be guessed likewise from its public-key.

iii.Algorithm of SHA3 -512

The SHA-3 hash function application incorporates three brands: initialization, absorbing and lastly squeezing. Initialization is purely the reseting of state matrix (A) ensuring all are zeros. In the absorbing stage, respective r-bit extensive block of the quality message is XORed that embraces the existing matrix state and 24 sucessive series of the compression assigned task are executed. The complete SHA-3 operation is the sponge operation depicted in Keccak [*r*, *c*] revealing that SHA-3 work with two functioning factors r is the message absolute size and *C* signify capacity, having the default as r+ *c* = 1600 bits. Likewise, RC

error "% 1 is not a valid output length ". n
end if "
m: = messagetobytes (message, messagetype);

Step 3.2 Generated capacity likened twice output length

The peer enrollment phase ensured generated CIC incorporation with the peer IP address while assuring secured communication ultimately on the network , denying unregistered malicious peer access in the peer-to-peer system. The sensitive nature of this peer-to-peer system inhibit malicious peer activities and simultaneously, displaying error on attempting to illegally connect to the network. Substantially, assuring security against any menace. The various experiment carried out but not limited to these ones illustrated in fig 2, fig 3, fig 4, fig 5 and fig 6. Securing the communication entails encrypting, subsequent decrypting of messages at both source and target peer respectively. Secure hash algorithm was implemented as additional security in this study

We actualized this result by indicating the public key encryption, message to be encrypted is typed and clicking on the send message button, encryption is effected. We decrypted this encrypted message by utilizing the private- key of the recipient peer. The process of effecting this necessitate clicking on the private key button and a key is systematically generated, inputted into the provided box and tick use private key decryption. The encrypted message is highlighted and clicking on the button with view decrypt, the encrypted message is decrypted promising security. This study provided additional security for the peer-to-peer communication as illustrated in figure 4.9. 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.

symbolizes the Round Constant . It will substantively provide SHA3-1024 capability in protecting the system [19] affirmed that the constants r[x, y] with RC were cyclical adjustable offset and iteration constant separately and were stated in this circumstance.

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

l: = keccak (m, 1600, 1600 – 2. n, n, hash):
bytestohexstring (l)
Step 4 Terminate process
End proc:

4. EXPERIMENT AND RESULTS

Fig 2: Ordinary Peer Disconnected Status with Additional Security

Fig 3: Secured Peer Communication Public Key Encryption

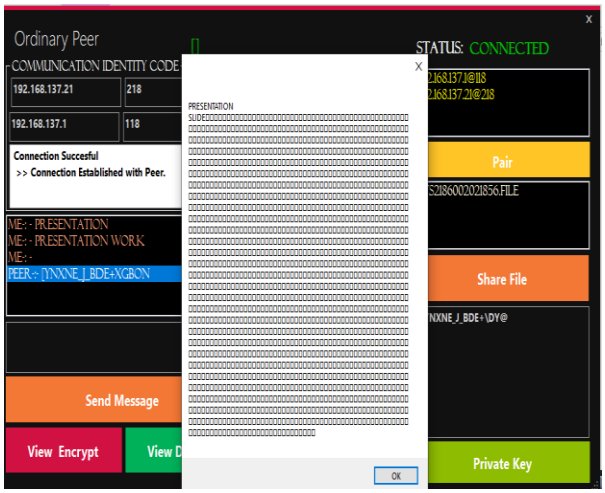

Fig 4: Secured Peer Communication Private Key Decryption

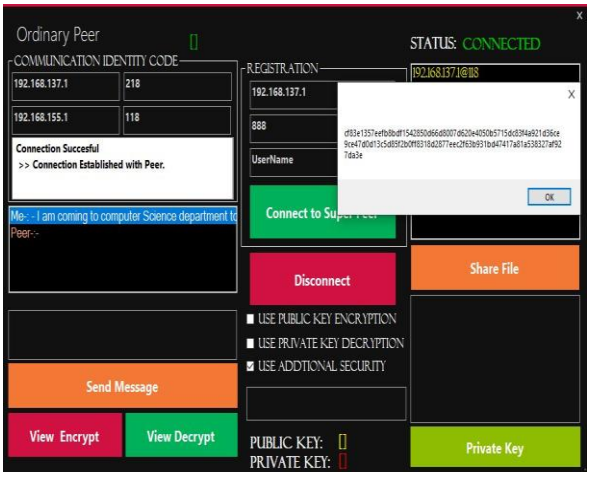

Fig 6: Peer communication generated hash message equival

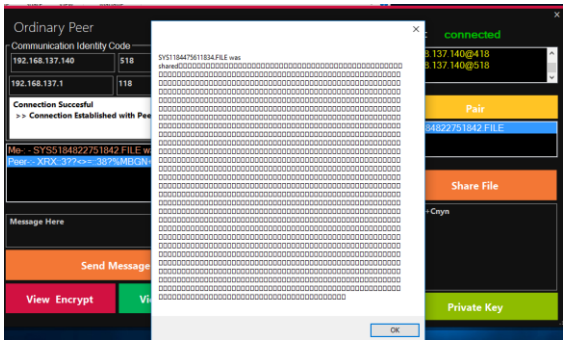

Fig 5 Peer Decrypted Using Share file

Table 1: Various Crptographic display of secure Peer Communication

Peer Types	IP Addresses	CIC	Port ID	Status	Peer Pair Connection With CIC	Secured Encrypted/ Decrypted Message	Secured Encrypted/Decrypted shared
Super Peer	192.168.137.1		888	Connected			
Peer 1	192.168.137.1	@118	888	Connected	Established	Encrypted/Decrypted	Encrypted/Decrypted
Peer 2	192.168.137.21	@218	888	Connected	Established	Encrypted/Decrypted	Encrypted/Decrypted
Peer 3	192.168.137.62	@318	888	Connected	Established	Encrypted/Decrypted	Encrypted/Decrypted
Peer 4	192.168.137.71	@418	888	Connected	Establishe-+*9d	Encrypted/Decrypted	Encrypted/Decrypted
Peer 5	192.168.137.140	@518	888	Connected	Established	Encrypted/Decrypted	Encrypted/Decrypted
Peer 6	192.168.137.142	@618	888	Connected	Established	Encrypted/Decrypted	Encrypted/Decrypted
Peer 7	192.168.137.165	@718	888	Connected	Established	Encrypted/Decrypted	Encrypted/Decrypted
Peer 8	192.168.137.174	@818	888	Connected	Established	Encrypted/Decrypted	Encrypted/Decrypted

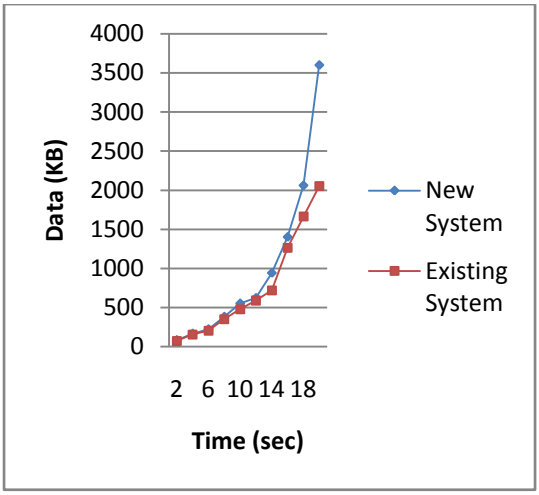

Figure 7: Graph of the encrypted data plotted against encryption

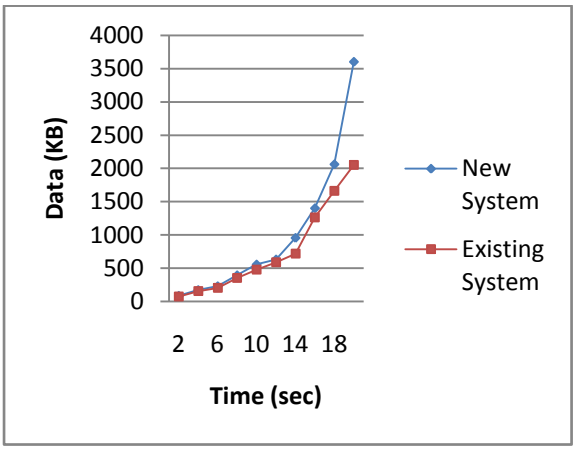

Figure 8: Graph of the decrypted data plotted against time forthe new and existing systemstime for the new and existing systems

5. RESULT DISCUSSION

The effect of our practical description on secured encrypted/decrypted message and share file is in Table 1. The concept is to deprive un-intended recipient from receiving the messages or file. 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 file utilizing encryption and decryption button in the system. This table is a furtherance of the first deliberated effect and this secured peer-to-peer system from the tables demand peers to communicate, likewise decrypt exchanged information through their generated CIC and private keys respectively. The figures in the table were the multiple effect portrayed in the course of testing the system workability. We attached some of the test done to ascertain our findings.The graph depicted in figure 7 symbolizes the time taking to encrypt feedback messages in the new system was substantially lesser than the time taken in the existing system.Lastly, the graph shown in figure 8 likewise demonstrated that the decprytion time adjudged from the new system was negligible likened to that of the existing system.

6. CONCLUSION

This study presented a secured peer-to-peer system that incorporates peer collaboration using Communication Identity Code , pursuit of tasks and content accessibility towards effecting desired goals. The procedure encourages peers to stipulate , exercise their interest interchanging information in a secured arrangement. The effectual and reliable peer user preference is assured with information or message protection in this framework. Inference drawn based on this work realistically provided security in modeling secured agent peer-to-peer system in execution time and can be expedient in a real world peer-to-peer set-up. The effect from modeling an agent, secured peer-to-peer concept substantiated this systematic coordination and improved peer-to-peer arrangement, ultimately affirming peers interest with secured feedback communication. Also, modeling a secured agent-based peer-to-peer system offered better capability, having embraced extended RSA, devoid of peer single point of flop, reassuring reliability, fortified and likewise guaranteed high quality performance This peer-to-peer system is robust and effectual in solving real world challenges that entail information exchange.

7. REFERENCES

[1] Androutsellis -Theotokis, S., and S. Diomidis. (2004). A survey of peer-to-peer content distribution technologies, In ACM Computing Surveys, 36(4):335–371.

[2] Moore, D. and J. Hebeler (2002) . Peer-to-Peer: Building Secure, Scalable, and Manageable Networks.

[3] *William. S* (2014).Computer Security, Third Edition http://williamstallings.com/ComputerSecurity

[4] 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.

[5] Mohammed. A and P. Annapurna (2012). Implementing a Secure Key Issuing Scheme for Communication in P2p Networks, International Journal of Wireless & Mobile Networks, 4,1.

[6] 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.

[7] Beverly,Y., and G. Hector (2003). Designing a Super-Peer Network. Proceedings of the 19th International Conference on Data Engineering, 1063-6382.

[8] Ehsan. S and M. Shahriar (2012). Anonymous Communication in Peer-to-Peer Networks for Providing more Privacy and Security,International Journal of Modeling and Optimization. 2, 3.

[9] Gulshan K, S.Anjala and S.Jyoti (2014). Authentication Techniques in ComputerNetworks,International Advanced Research Journal in Science, Engineering and Technology1, (2).

[10] Hexmoor.H and S.Nagalakshmi(2016). Enhancing Reliability in P2P Networks Using Social Capital Principles, Journal of Networks and Systems, 5,(1).

[11] Kasyful. A (2017). Collaborative File Sharing System Using Jxta P2p Networking Infrastructure – AnApplication Development , Journal of Environmental Engineering & SustainableTechnology, 4 (1), 31-40.

[12] Kayalvizhi .K and R.Bharathi(2014). Efficient and Distributed Network Model for Peer-to-peer Systems, International Journal of Computer Science and Mobile Computing, 3, (2), 626-632.

[13] Keong.L, C. Jon ,P. Marcelo ,S. Ravi and L.Steven (2004). A Survey and Comparison of Peer-to-Peer Overlay Network Schemes, IEEE Communications.

[14] Khalid .K(2015).Mobile Agent: A Comparison Review, International Journal of Computer ScienceandMobileComputing,4,(7),122-127.

[15] Rajeev Sobti and G. Geetha (2015). Performance Comparison of Keccak, Skein, Grøstl, Blake and JH: SHA-3,Final Round Candidate Algorithms.International Journal of Security and Its Applications ,9, (12),367-384.

[16] Rajesh.K, P.Suman and K.Vinod (2016). A Survey of Peer-to-Peer Networks, International Journal of Advanced Research in Computer and Communication Engineering.5, (4)

[17] Xu.Y, C. Deng and M. Gao (2012).The Topology of P2P Network, Journal of emerging trends in computingand information sciences.,3 ,8 , 2079-840

[18] Arvind, N., J. Bonneau, F.Edward, M. Andrew and G. Steven.(2015) . Bitcoin and Cryptocurrency Technologies, Princeton Pu Ltd, USA.

[19] 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.