Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.12, No.2, 2021

A Secured Agent-based Model for a Peer-to-Peer System

Jude Opuh[1], Bartholomew Eke[2], Edem Williams[3]*

1,2. Department of Computer Science , University of Port Harcourt , Rivers State, Nigeria

3. Department of Computer Science, University of Calabar , Cross River State, Nigeria

* *E-mail*: jude.opuh@yahoo.com

Abstract
In this paper, 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.
Key words : Peer-to-peer, Agent-based, Secured and Communication.
DOI: 10.7176/CEIS/12-2-03
Publication date: May30th 2021

I. Introduction

The advent of peer-to-peer (P2P) systems, in the preceding years of persistent effort, have transformed the approach in disseminating information and technique in extracting information from collaborating or distributed systems. This peer-to-peer system is a deviation from the well-known client-server computation set-up. The 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. In this system, the user or client direct request or queries to any arbitrarily preferred peer and wait for a substantial response from the data sources kept in the entire connected network. These peers have similar functions with diverse liabilities. Koubarakis(2003) revealed that peers co-operate in sharing or consuming services including resources with one another. The topology in a peer-to-peer system signifies the manner its peers will be positioned on the partial network. 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.

The distributed system is taken to be a pure peer -to -peer, in the first instance if it is a peer -to -peer network, secondly if any arbitrary solely selected terminal entity is isolated from the network devoid of having the system experience any loss of likely network service. The peers partaking in this kind of set-up are clearly resource (service and content) suppliers and also resource (service and content) collectors (Servent -concept). Oram(2001) prior to 1999, peer-to-peer was a subject of research concern to only the researchers, however the emergence of Napster in earlier mentioned year brought reform and sensitivity regarding peer-to-peer research. Androutsellis-Theotokis(2004) 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.
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.

Kurose and Ross (2003) said that this peer is termed bootstrapping node and expected to be steadily available online. It is worth stating that Fast-track client, in an instant Kazaa is implemented on a peer, the bootstrapping node will be communicated to establish if the peer is justified to be called a Super node hence will be availed with some or entire IP address of the Super nodes. Juan and Zheng (2012) said the motive that gave birth to the desire for an improved standardized shared data plan for data communication and integration among

heterogeneous applications and structures are the merits of interoperability, demonstrated through the web (Papamarkos et al 1998).

The major causes of these attacks that makes them effective is due to the design installed in today's Internet. The Internet is intended for speed in sending of packets and gave less attention to the contest of security. Gancheva et al (2011) declared that the database acquired from the various scientific study were typically heterogeneous and dispersed.The commitment in ensuring protection of information in Internet was kept for individuals supplying and demanding this information.

The successful connection to the network by a malicious peer provide an easy entrance to persuade its other accomplices connecting straight to the network devoid of having to influence further the non-malicious peer. 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 networks of peer-to-peer. In this framework, it is anticipated that each peer is meant to possess private/public dual key 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.* The problem of hijacking connection by malicious peers in a peer-to-peer network constitute our statement of the problem in this paper.

2. **Literature Review**

Ghassan and Graham (2013). worked on the Generic modelling of security awareness in agent based systems and recommended that agents are encouraging software developing blocks in constructing precise information in distributed systems. This is devoid of a security-related need, however, it still incorporates security-related operations as an agent is likely to send a genuine request to peers it has earlier communicated with authority to establish a community.

DaeSu et al (2003) deduced in this study that the forming, planning of an agent system with the desire to realize their set goal, prompted various brands of agents that revealed rational characteristics. These incorporates the main, managing, watching, reporting and application agent. The study discussed modeling and creation of an agent system as both circumstance yielded reasonable intermediate substantial outcome.

Marcus et al (2013) tried working on the client's interactive behaviour to design peer selection policies for Bit torrent-like protocols. The consequence of this study assured workloads of genuine content suppliers and examined these dispersion benchmarks herein stated: temporal, spatial e.t.c.

Ghada et al (2011) worked on the Domain-based query routing mechanism for peer-to-peernetworks, as in the latest years, peer-to-peer framework is extensively embraced by both academic and industries. Finally, it is assumed that the Domain-based probing routing framework can effectually and excellently aid request processing in a vast domain peer-to-peer information sharing arrangement.

Rozita et al (2014) researched on *a* comprehensive survey of Intelligent Agents. The agent known in computer science is a software or any other operational entity possessing some intelligent qualities . Also, various predominant descriptions of intelligent agents incorporated with numerous use of intelligent agents was deliberated, discussion on self-directed agents and various implementation of the agents were conspicuously studied.

Senthil et al (2016) researched on the particle swarm optimization (PSO-based) peer selection approach for highly secure and trusted peer-to-peer system. Their later work is to advance the quality in the peer-to-peer concept for the social media programs.

António and Luís (2008) focused on improving multi-agent based resource coordination in peer-to-peer networks Finally, their result was impressing, having relied on creating , employing sophisticated efficient search mechanisms that dynamically generate , takes advantage of a network of semantic dependencies between peers and its resources. Khalid(2015) *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 . Consequently,they asserted that mobile agents can be effectively used in gathering, filtering, sharing,*

monitoring, recommending, comparing and guiding information Xiao-Long et al (2016) worked on hybrid collaborative management ring on mobile multi-agent for cloud-peer-to-peer. Substantially, their study utilized the mobile multi-agent technology to construct an effective hierarchical integration model named cloud peer-to-peer. Subsequently, after in-depth analyses and experiment, the hybrid collaborative management ring based on mobile multi-agent depict a significant improvement..KeeHyun and Joonsuu (2013) researched on designing of a monitoring system for many collaboration agents Substansively, their result revealed more efficient internal structure, message transmission methods in the agent and peer-to-peer host environment. 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 .Kayalvizhi and Bharathi(2014) researched on efficient and distributed network model for peer-to-peer systems, Finally, their result revealed that SORT can be adapted in various peer-to-peer applications

3. Materials and Method

3.1 Proposed System

The design of our proposed system is depicted in figure 1. It is the architectural design of an agent-oriented modeling of secured peer-to-peer system. This was in addition designed to demonstrate the progression of peer-to-peer communication The system permits peers seeking entrance to the network on fulfilling well defined conditions for enrollment to be analyzed for authenticity and systematic generation of communication identity code on satisfied enrollment completion.

effectual and secured system. The methology adopted in this study is Object –Oriented Analysis and Design methology as it explains the agent communication, flexibility as it guarantees ease of implementation and object interactionThe super peers incorporate with the agent for effectual coordination of the absolute peer-to-peer system. The agents attest that a peer conect just once to the network and simultaneously a communication identity code (CIC) is systematically generated, likewise the providing peer and respective CIC further serve as a proof of authentication for peers that legitimately wish to communicate in the peer-to- peer system. The proposed system embraced security in designing a hybrid peer-to-peer set-up incorporating agent concept and likewise creating a substantial amount of peers with limited super peers. Peer-to-peer arrangement can be proficiently tracked through respective IP addresses for file or significant content sharing, request initialization and feedback

Some security services like authentication and non-repudiation with agent incorporation are embraced in designing a secured peer-to-peer concept in this security domain of study.

The two security services that were previously stated assures efficiency and dependability in the peer-to-peer strategy and agent incorporation in attaining security goals.

Substantively, confidentiality, availability and integrity are also vital security services that will help in the security goals.

Agent Modules. The different agent modules that was utilized in designing this system performed crucial role in creating an effectual and secured peer-to-peer communication set-up. These roles incorporate surveillance agent module meant to aid peer enrollment and execution of integrity check on resources /files that a connecting or re-connecting peer is offering to the system, mobile agent module, coordinating agent module and compliance agent module e.t.c.

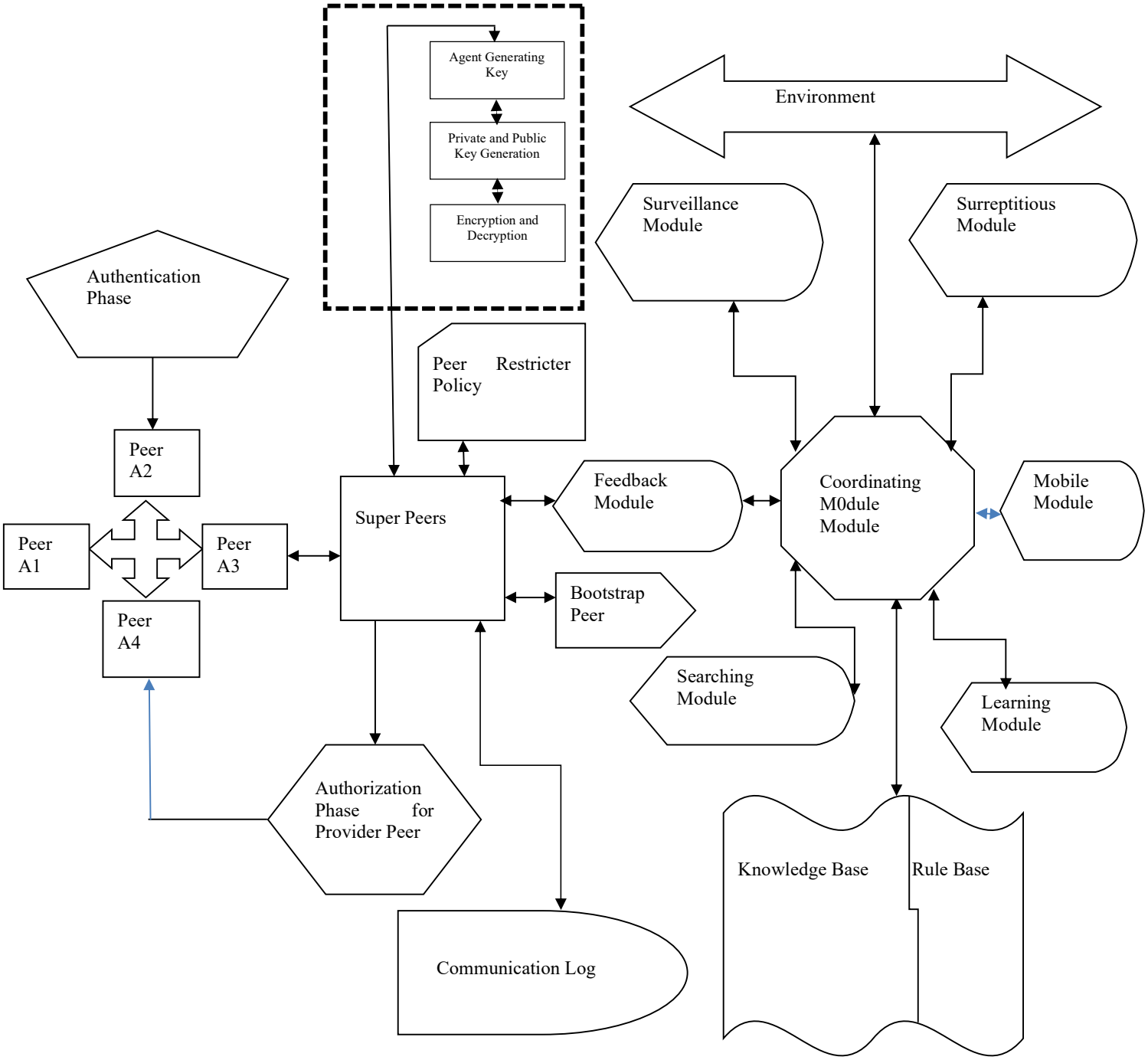

Figure 1 Detailed Model of a Secured Agent Peer-to-Peer System

3.2 Algorithm for Peer Registration in the Proposed System

Input: IP Address and likewise Port Number of Super Peer.

Output: IP Address of Ordinary Peer and CIC.

Step 1: Create the Super Peer application platform.

Step 2: Start the Super Peer application platform.

Step 3: IP address of the Super Peer displayed.

Step 4: Create the Ordinary peer application platform

Step 5: Input generated Super peer IP address and port number into applicable box.

Step 6: Click connect to the Super Peer.

Step 7a: Output generated Peer IP address and likewise Communication Identity Code.

Step 7b: Repeat this procedure for multiple peer enrollment as required, otherwise if enrollment exercise is over, go to step 7c.

Step 7c: End enrollment process.

Algorithm for Secured Peer–to-Peer Communication in the Proposed System

Input: Pair the IP Address and CIC of intending peers to communicate.

Output: Display messages of Secured peer-to-peer communication.

Step 7a- 1 (Start): Pair the two intending peers for communication with their IP and likened CIC.

Step 7a-2: Generate respective messages to adjudge if communication is successful or failed.

Step 7a-2: If effect is successful, attempt to encrypt messages from an originating peer and Decrypt

likewise message utilizing the private key of a receiving peer.

Step 7a-3: Display the various effect.

Step 7a-4: Repeat likened procedure to share file utilizing an encryption and subsequent decryption button.

Step 7a-5: Display the effect.

Step 7a- 6: Output feedback messages of a secured peer-to-peer system

Step 7d: End the Communication Process

Knowing the peers providing service plays a substantial role in improving security and likewise avoiding purposeless search from requesting peer by flooding ample request and finally exposing the system to malicious menace.

This problem of lessening needless request of respective peers for information exchange is significant for both the peer requester and supplier.

There is necessity to improve on the existing system by ensuring an effectual, robust, reliable, secured peer-to-peer arrangement and this is accomplished utilizing agent concept

3.3 Agent Approach

Input: Modeling an agent.

Output: Effectual and secured peer-to-peer system.

Step 8-1 (Start): Create substantial number of agent modules with specialized name identitification.

Step 8-2(Register): Enroll desired agents for consistency and transaction update.

Step 8-3(Introduce): Introduce the security service goals in agents for system dependability.

Step 8-4 (Search): Agent searches , direct peers willing to be enrolled and conducting of relevant check for respective connecting or re-connecting peers in the system.

Step 8-5 (Update): Update where necessary peers appearance and disappearance at repective circumstance.

Step 8-5a (Authenticate): Agent ensure CIC generation and likened to authentication of peers for communication.

Step 8-5b (Generating key): Agent activate and realizes key generation in this peer-to-peer concept.

Step 8-5c (Confirmation): Agent ascertain if respective peer communication had a feedback effect in a secured and likewise displayed.

Step 8-6(Continue): Otherwise go to step 8-5b and attempt the procedure pending a satisfactory secured peer-to-peer communication feedback effect is realized.

Step 8-7: Display effect , affirming an effectual , robust , reliable and secured peer-to-peer system.

4. Experiment and Results

It is important to state that the enrollment phase is the most imperative phase in this peer-to-peer system., The super peer run function, permit start up, connect and likewise generates its IP address. The ordinary peer concept initially displayed disconnected status, on meeting set criteria connect to the super peer with port identity for systematic generation of its IP addresses on connecting to the super peer and automatically display connected status. These are depicted in figure 2, figure 3, figure 4 , figure 5 and figure 6. This peer-to-peer system is modeled to accommodate large number of peers ready for connection and communication with robust and added security. The absolute idea in this peer enrollment phase is to ascertain the peers that will be connecting to the network for detailed planning as the network expands with peer activities. Likewise, this 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. Peer enrollment phase assure peers with connection successful as demonstrated for permission to exchange information with respective peers and substantively ensure authentication and non-repudiation. In the secured peer communication phase, it is envisaged that the interacting 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

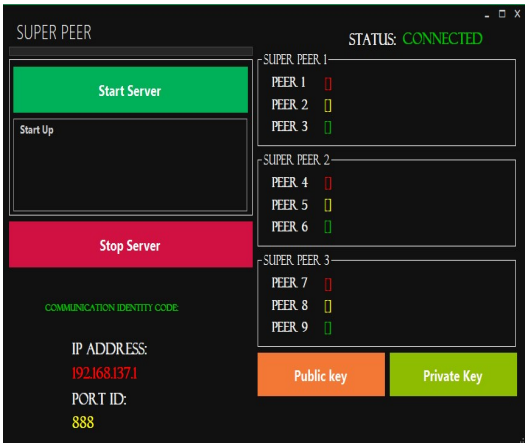

Figure 2: Super Peer Connected Status

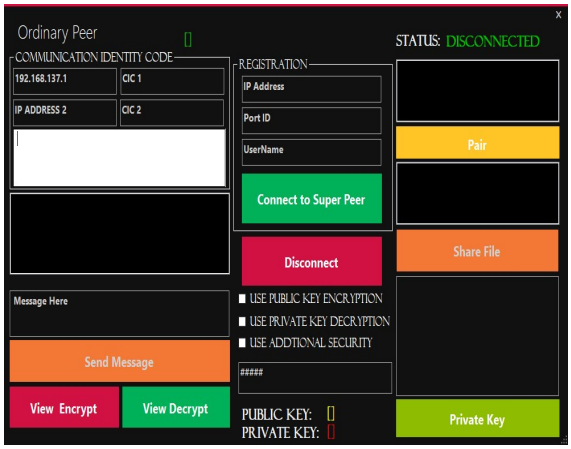

Figure 3 : Ordinary Peer Disconnect with additional security

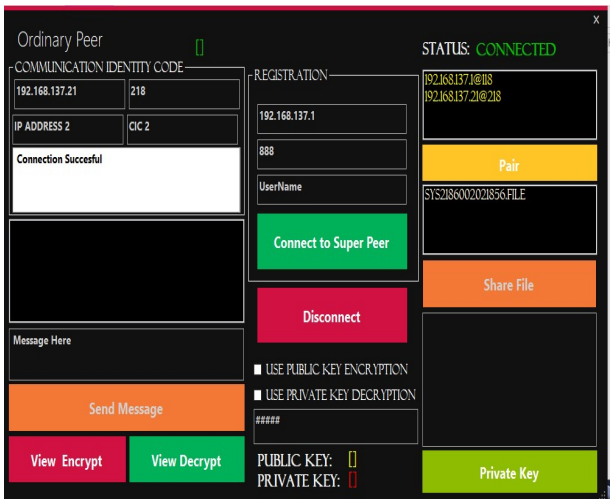

Figure 4: Ordinary Peer Connected Status IdentityCode

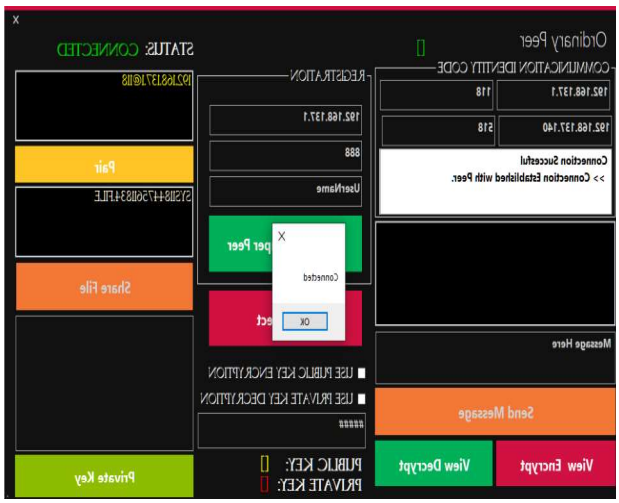

Figure 5: Peer Pair Connection with Communication

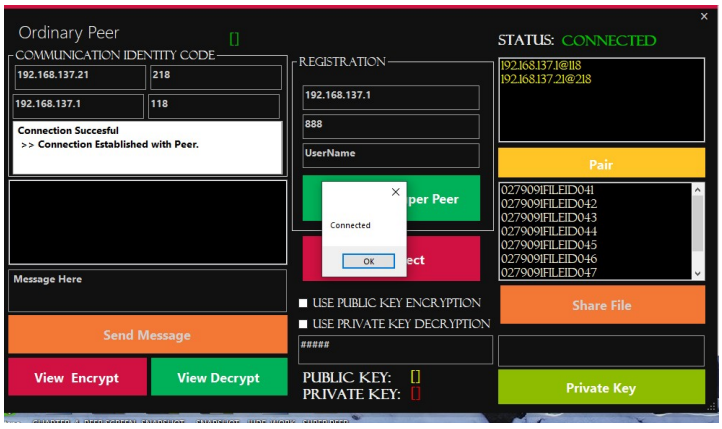

Figure 6 : Peer Pair Connection with Communication Identity Code (218)

Table 1: Various peer pair connectivity and communication display

Peer Types	IP Addresses	CIC	Port No	Status
Super Peer	192.168.137.1			Connected
Peer 1	192.168.137.1	@118	888	Connected
Peer 2	192.168.137.21	@218	888	Connected
Peer 3	192.168.137.62	@318	888	Connected
Peer 4	192.168.137.71	@418	888	Connected
Peer 5	192.168.137.140	@518	888	Connected
Peer 6	192.168.137.142	@618	888	Connected
Peer 7	192.168.137.165	@718	888	Connected
Peer 8	192.168.137.172	@818	888	Connected

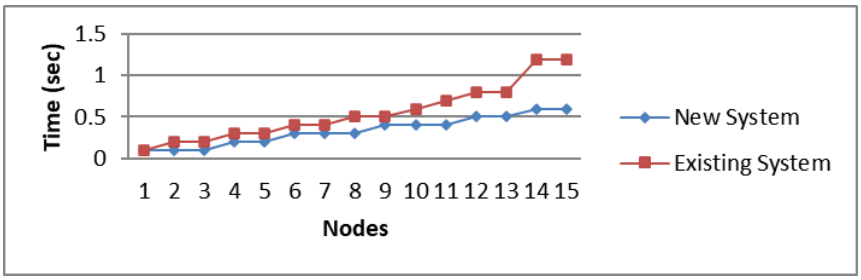

Figure 7: Graph of connectivity/node discovery in the new system compared with the existing system

5. Result Discussion

The communication and likened activities in peer–to-peer arrangement incorporates changes dynamically and taking security into consideration .This necessitated an agent concept in a secured peer-to-peer system, creating robustness, effectual, reliability and taken into cognizance some indices like IP address, CIC, connection status and this is enabled to run in the proposed framework of secured peer-to-peer as depicted in Table 1. We tested respective indices in ensuring adherence to the system arrangement and peer forms, for instance the super peer as a peer type will be started to connect on the network, requiring its IP address with respective port number to be portrayed else the process should be attempted until a successful start of the super-peer is established on the network.

The ordinary peers as the second peer type, likewise connect to the network for systematic peer enrollment by inputting the already displayed IP address, port number of the super peer and clicking connect to the super peer automatically generate CIC for multiple number of ordinary peers with peer status revealing connected. The generated CIC ensure peer pair without this code respective peers cannot connect to the super peer network.

The graph describes the time taken in the system for nodes to connect in the network likened to the existing system is shown in figure7. The time for discovery of connected nodes in this new system was less than the time of similar nodes discovery on the existing system.

6. Conclusion

Securing peer-to-peer communication and information exchange is a critical issue that must be countered in order to accomplish a reliable and effectual secured system that is consistently fortified. In furtherance, owing to the distributed, dynamic and malicious behaviour in peer activities, a secured peer-to-peer system still persist as a resilient area of research and likened to the continuing upward trends in peer incorporation with similar

functionalities. This peer-to-peer system was systematically modeled to control peer activities with secured communication, assuring security goals and optimal ssystem fortification.

References

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

António. L and B. Luís (2008) .Improving Multi-Agent Based Resource Coordination in Peer-to-Peer Networks.Journal of Networks, 3,(2)

Charu V.(2012).A Comparison of Communication Protocols for Mobil Agents,International Journal of Advancements in Technology, 3. (2.) .

DaeSu, K., S. Chang and R. Kee (2003) . Modeling and Design of Intelligent Agent System, International Journal of Control, Automation, and Systems, 1, 2,

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,

Ghada, H., I. Hamidah , S. Md.Nasir and Y. Rasali (2011). A Domain-based query routing mechanism for peer-to-peer networks, The 8th International Conference on Mobile Web Information Systems, Procedia Computer Science 5 , 578–585

Ghassan, B and L.Graham (2013). Generic modelling of security awareness in agent based systems in Information Sciences.

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.

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

Koubarakis, M. (2003). MultiAgent Systems and PeertoPeer Computing: Methods, Systems, and Challenges. Proc. CIA, Springer LNCS 2782. 46-61.

Kurose, J .and K.Ross (2003). Computer Networking: A Top-Down Approach Featuring the Internet, Addison Wesley, Boston.

Marcus,V., M.Rocha1 and K .Carlo (2013). On Client's Interactive Behaviour to Design Peer Selection Policies for Bittorrent-Like Protocols, International Journal of Computer Networks & Communications ,5, (5).

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.

Pang, X., B. Catania and K. Tan (2003). Securing your data in agent-based P2P systems. In Eighth International Conference

Papamarkos, G., L. Zamboulis and A. Poulovassilis,(1998) , XML Databases, School of Computer Science and Information Systems,

Oram, A. (2001). Peer to Peer: Harnessing the Power of Disruptive Technologies.

Rozita ,J., N. Hamidreza and S.Zahra. (2014) . Intelligent Agents: A Comprehensive Survey,International Journal of Electronics Communication and Computer Engineering Volume 5, (4), 2278–4209.

Senthil, M, T. Revathi and Nallakannu (2016). PSO-based optimal peer selection approach for highly secure and trusted P2P system. Security Comm. Networks; 9, 2186–2199.

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.

KeeHyun .P and P. Joonsuu (2013). Design of a Monitoring System for Many Collaboration Agents, Journal of Advanced Science and Technology , 35,.7-10