An Efficient system for improved throughput and delay over VOIP

Omesh Kalambe[1], Bhagyashri Pokale[2], Ashwini Meshram[3]
[1]Assistant Professor, Department of Computer science & Engineering, GHRIET, Nagpur (MS), India.
[2,3]Resesrch Scholar, Department of Information Technology, GHRIET, Nagpur (MS), India.

Abstract— *Voice over Internet Protocol (VoIP) is a growing Communication and Information technology that assists voice communication through the Internet. VoIP is becoming popular due to their cost valuable service and convenience. A VoIP technique has two significant features i.e. Privacy and QoS of the network. Unfortunately, most VoIP network doesn't offer Privacy as well as QoS to the user. A work has done before on Security and Quality of Services for VoIP applications, yet these issues has not been completely solved. To overcome these issues in VoIP proposed a novel Advanced Encryption Standard (AES) and Secure Hash Algorithm -1 (SHA-1) for Client-Server model. Here, AES and SHA-1 are use to afford secrecy.*

Keywords-*QoS, VoIP, SHA-1, AES***.**

I. INTRODUCTION

Internet Protocol Telephony (IP telephony) is a technology which provides voice communication over the network. It conduct telephone call using packet switch base network. It is also known as "Voice over Internet Protocol (VoIP)". It is design to swap traditional circuit switched based network.[1]

In VoIP travels call as a packet of data. The task in VoIP is to transport speech packet in a reliable stream. The chief benefit of IP telephony is that long distance call is also on regular cost. VoIP is a significant quantity of the union of telephones and computers into a solitary united information atmosphere. There are many protocols for anonymity, we will specify their common limitations to justify our choice for an anonymous hybrid P2P model. Before delving into the literature review, we need to highlight that although the concept of mixing is commonly used for privacy, but this technique does not work for VoIP since during the setup of VoIP the source identity is stated in the RTP header, and the timestamp allows the attacker to correlate pairs[2].

There are various issues of VoIP such as delay occurs during packet transmission process from source to destination that is main issue which needs to recover. Second issue is, more variation occurs in the delay among successive packet i.e. Jitter. Third is the throughput of the system is less. Fourth is rate of packet loss is high. Packet receiving excessively late at the receiver side [6] . Echo sound is also generated during conversation. Frequent disconnection among sender and receiver [3].

Client-Server model is stated as a networking computing prototypical in which all services and request are delivered over a network. In this model computer is act as either client or sever. Client computer execute application on it. A server is a dominant computer offers and accomplishes the services and resources which are consumed by the client. Depending on the environment of application we can conclude which computer act as a client or a server or both.

Using Internet connection one or more client computer connected with server. As per client demand server offers high-end computing exhaustive services. For communication, Clients and servers interchange messages in a request-response pattern. Request is send by client and server proceeds a response respective to the client request. This interchange of message is like inter process conversation [10, 11, 12].

Objective of the system is to study numerous qualities of services which are provided and secrecy concerns in VoIP and their effect on the communication data.Secondly, Study several technologies to overcome VoIP glitches and implement more effectively in our VoIP network. Also, to develop durable connection between source and destination for reliable data transmission.

II. LITERATURE SURVEY

Many researchers have worked on Secrecy and Quality of Services (QoS) disputes in VoIP network to address numerous restrictions. In this sections several techniques have been studied which is used in VoIP. Security as well as Preserving QoS of the network is major challenging task in VoIP system.

Wireless LAN (WLAN) is the fundamentally structured wireless technologies all over the world. WLAN architecture is equivalent to Local Area Network (LAN) but communication ensues in WLAN by Radio frequency (RF) or Infrared (IR) and by physical lines in LAN. Cost

effectiveness, Simplicity, Scalability and Mobility are the main characteristics in WLAN. WLAN carries association using IP and VoIP applications are also successively running through Internet Protocol [2].

2.1 Hybrid Network:

Hybrid network determination in VoIP is to offer security for VoIP system. Hybrid network is able to afford safety for high latency conversation via routing network traffic. Offering of quality of services desirable in hybrid network it is unable to offer both secrecy as well as quality of services at a time. An example of this is a network that combines wired and wireless technologies. It can additionally consult with a network style that mixes 2 or additional kinds of basic physical topologies, such as multiple star topologies connected by a bus topology.

Here, user plays a router roll which obscures the scheme. Also, it is accountable to disruptions the perception of sharing work on the unalike element of the network. Moreover low latency applications on unify network may be susceptible to Timing Analysis Attack [1,3].

2.2 Peer-toPeer Network:

In peer-to-peer (P2P) network, two or more PCs are connected which share resources without going through a separate server computer. A P2P network can be a poster hoc connection—a few computers connected via a Universal Serial Bus to transfer files This P2P frequently involves of a core proxy and a fixed of patrons that are attaching to the brink of this core proxy. In P2P, each user acts as a client and server. Therefore any one of these two exposes its identity then entire network will be insecure [2].

2.3 Authentication Techniques:

The first most important step for securing a computer system is the ability to verify the registered user. The process of verifying a user's identity is typically referred to as authentication of the user. Passwords are the method used most often for authenticating computer users, but this approach has often proven insufficient in preventing unauthorized access to computer resources once used as the sole means that of authentication

In network, authentication is the most important phenomenon respites to distinguish and remove any dishonest network accessory. For IEEE 802.11s and 802.11i centralized server is obligatory for authentication phase. But, centralized server endeavors as a third party. It also inhibits discrete activities and thus suffering scalability concerns [5].

III. PROPOSED SYSTEM

The study understood voluminous systems are wont to answer key options in VoIP, But these problems have not been completely resolved. This problem is confiscate victimization permutation of SHA and AES.

There are four different types of SHA algorithms are named SHA-0, SHA-1, SHA-2, and SHA-3.It is a cryptographic hash operate. I used SHA-1 for authentication which generates a a hundred and sixty bit hash worth.

Its hash value is normally extracted as a hexadecimal number. SHA-1 is working in various extensively used applications.

The Secure Hash Algorithm (SHA) was designed by the National Institute of Standards and Technology (NIST) along with the NSA (National Security Agency) to be used with the Digital Signature Standard. SHA was modelled closely after the MD families of message digest algorithms developed by Rivest. SHA takes a 512 bit input and produces a 160 bit output. SHA also has a 160 bit Initialization Vector (IV) which can be modified but there is a standard setting for this vector which is believed to give good security. SHA was designed to make the process of digitally signing messages more practical [13].

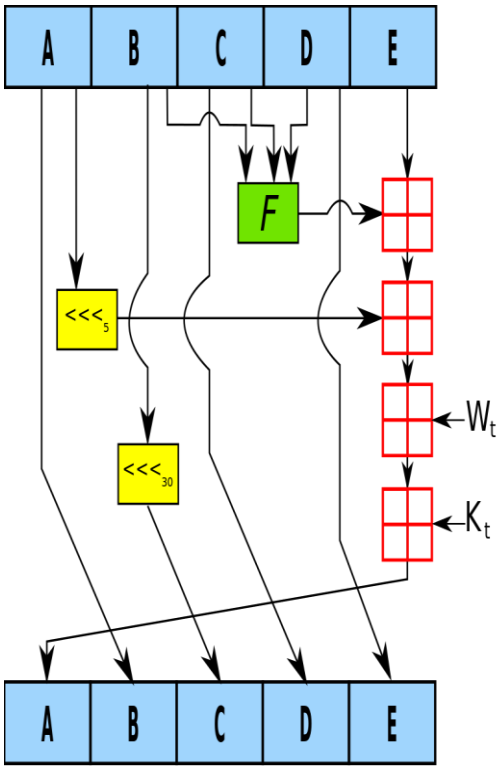

Fig 1: Secure Hash Algorithm (SHA 1) [15].

3.1 Advanced Encryption Standard (AES):

The symmetric key rule that releases to cipher and rewrite the information . AES bids key sizes are of 128, 192 and 256. The data is delivered through N stages for encryption. And these stages are shuffle as per the key size. Fort 10 stages key size is 128 bit. If the stages are 12 and 14 then key sizes are 192 and 256 separately. These all rounds or stages are administrated via four modifications i.e. SubByte, ShiftRows, MixColumn and AddRoundkey [7,8,10].

As per the key size these rounds are shuffle. When the structure is 10 then key size is 128 bit. For 12 and 14 structures key sizes are 192 and 256 in turn. These stages are rapt via four amendments i.e. SubByte, ShiftRows, MixColumn and AddRound key 10].

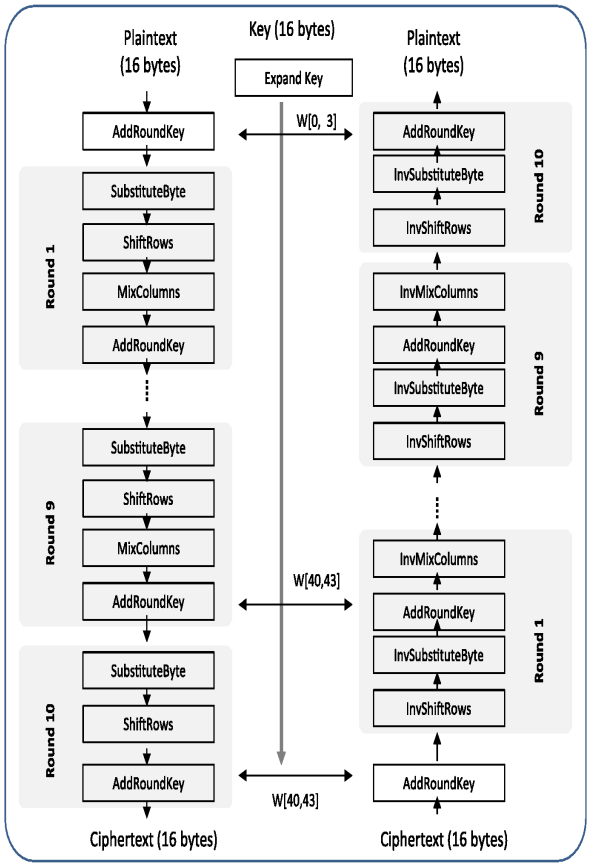

Fig 2: Advanced Encryption Standard (AES) [16].

IV. Experimental Results

To improve in quality performance of services parameter and security issues in VoIP using client-server network, is implemented for real time application on hardware module i.e. Peraonal Computer or Laptop. The setup will consists of one client machine and one server machine with JDK1.6 installation. A server having its own database and client registered with it. The setup also requires microphone through which communication is perform. The researcher implemented database system in MYSQL.

Results shows the performance of proposed system with existing system related to Throughput, delay and jitter. Delay and jitter of the proposed system must be minimum compared with existing system.

Delay and jitter are shown in figure in milliseconds. Jitter is a general problem for the connectionless networks of packet switched. The information (voice packets) is divided into packets; each packet can travel by a different path from the one end to another. Jitter is one of the most common VoIP call quality problems. For better throughput jitter should be minimum. Delay is caused when packets of data (voice) take more time than expected in order to reach their end. This causes some disruption is the voice quality. However, if it is treated properly, its effects can be minimized. Delay of the proposed system should be minimum.

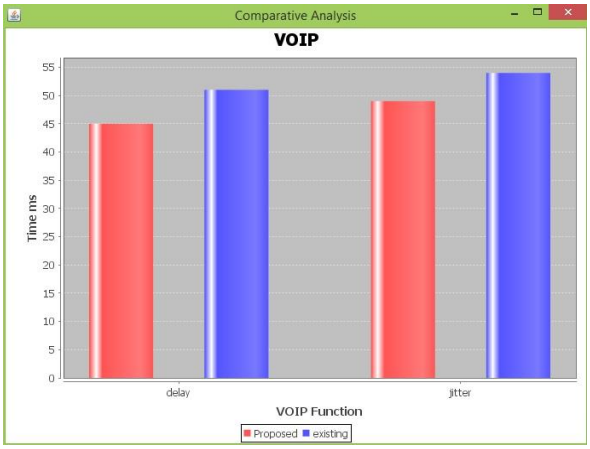

Fig 3: Delay & Jitter

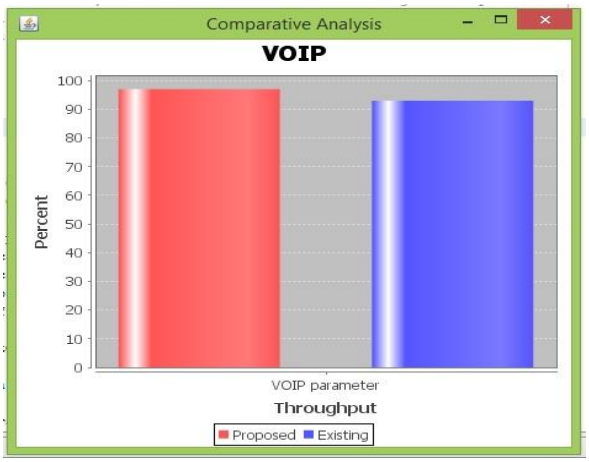

Fig 4: Throughput

V. CONCLUSION

VoIP attendances vast complications for real time transmission application. To afford applicable stability among quality services and privacy problems is that the central half in VoIP preparation. The propose work incontestable through an experiment additionally as analytically to preserve QoS and Secrecy disputes in VoIP. It maintains acceptable steadiness among Secrecy additionally as QoS problems that is crucial for any VoIP application preparation. Also, management of is superior than transmission control protocol related to to outturn once quantity of flows is extraordinary.

REFERENCES

[1] Zahraa Sabra and Hassan Artail, "Preserving Anonymity and Quality of Service for VoIP Applications over Hybrid Networks," 17th IEEE Mediterranean Electro technical Conference, Beirut, Lebanon, 13-16, April 2014.

[2] K. Bharathkumar, R. Premalatha Kanikannan, Dr.Rajeswari Mukesh, M.Kasiselvi, T. Kumanan, "Privacy Preserving of VoIP against Peer-to-Peer Network Attacks and Defense," International Journal of Computer Network and Security (IJCNS) Vol 4. No 1. Jan-Mar 2012 ISSN: 0975-8283.

[3] Mudhakar Srivatsa, Ling Liu and Arun Iyengar, "Preserving Caller Anonymity in Voice-over-IP Networks," 978-0-7695-3168-7 /08 $25.00 © 2008 IEEE.

[4] Mudhakar Srivatsa, Arun Iyengar, Ling Liu and Hongbo Jiang, "Privacy in VoIP Networks:Flow Analysis Attacks and Defense," IEEE INFOCOM 2009.

[5] Celia Li and Uyen Trang Nguyen, "Fast- Authentication for Mobile Clients in Wireless Mesh Networks," 978-1-4244-5377-1/10/$26.00 ©2010 IEEE.

[6] Abdi Wahab, Rizal Broer Bahaweres, Mudrik Alaydrus, Muhaemin, Riyanarto Sarno, "Performance Analysis of VoIP Client with Integrated Encryption Module," 978-1-4673-2821-0/13/$31.00 ©2013 IEEE.

[7] Pallavi Gangurde, Sanjay Waware, and Dr. Nisha Sarwade, "Simulation of TCP, UDP and SCTP with constant traffic for VOIP services," Vol. 2, Issue 3, May-Jun 2012, pp.1245-1248.

[8] http://toncar.cz/Tutorials/VoIP/VoIP_Protocols_Introducing_H323.html.

[9] http://www.telecomspace.com/vop-h323.html.

[10] http://www.networkworld.com/article/2332980/lan-wan/what-is-sip-.html.

[11] http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-1/s.

[12] http://www.en.voipforo.com/SIP/SIP_architecture.php.

[13] Monjur Alam and Sonai Ray,"Design of an Intelligent SHA-1 Based Cryptographic System: A CPSO Based Approach", International Journal of Network Security, Vol.15, No.6, PP.465-470, Nov. 2013,pp no 465-470

[14] Pallavi Gangurde, Sanjay Waware, and Dr. Nisha Sarwade, "Simulation of TCP, UDP and SCTP with constant traffic for VOIP services," Vol. 2, Issue 3, May-Jun 2012, pp.1245-1248.

[15] https://en.wikipedia.org/wiki/SHA-1#SHA-0

[16] https://www.google.co.in/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwiKgbzx0bLSAhXLlJQKHVp3Bx4QjRwIBw&url=http%3A%2F%2Fopticalengineering.spiedigitallibrary.org%2Farticle.aspx%3Farticleid%3D1863832&psig=AFQjCNHeTY8VIkvBV1o9MF5f6LYTO6beGw&ust=1488366071531470