International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2019.3389

E-ISSN : 2454-6135

Volume.5, Issue 2
February -2019

Implementation of Secured Portable PABX System of Fully Fledged Mobility Management for Unified Communication

Md. Torikur Rahman[1] F.M.Rahat Hasan Robi[2]

Lecturer [1, 2]

[1]Department of Computer Science & Engineering

Uttara University

Dhaka, Bangladesh

[2]Department of Computer Science & Engineering

Bangabandhu Sheikh Mujibur Rahman Science and Technology University

Gopalganj, Bangladesh

ABSTRACT

Now is the age of information technology. World is advancing day by day. At present in this progressing world communication from one place to another has become so easy, less costly, and faster. This modern life is almost impossible with the help of these communication technologies. People need to talk, need to share data, need to express their emotion from long distance. So they need to use technologies to communicate with one another. Some software like Skype, Yahoo, Gtalk, and Msn is used for this purpose. But these software uses high capacity of bandwidth and a big amount of internet speed. Thinking of this, I propose a Secured Portable PABX System for Fully Fledged Mobility Management of Unified Communication that operates with local LAN bandwidth consist of three limited equipments-1) Server 2) Soft phone 3) Web cam. With this system people can make video call using low internet speed. It has unique extension number that gives access to the parties within a communicating session. It is possible to make video call through this system with lower cost and lower internet speed independent on operating system. The main advantage of this system is the portability of the system. It can run on both Linux and Windows operating system that makes it special. This system can be implemented on telecommunication sectors like call center, mobile phone customer care center etc. It also implemented in security issue like CCTV camera. Finally, this system is better because it has the ability to make calls in different extensions also has the ability to show video calling with conferencing, web conferencing and presentation articles at a time within a conference session.

Key Words: *PABX, SIP, LAN, Security, DoS, Encryption*

1. INTRODUCTION

Now at the age of information technology, virtual and existing systems are filled through the communication market because of different stand-alone servers. With these systems people, can communicate through ease sitting their home instead of large systems and going outside. Thinking at the existing system, a unified communicative portable PABX system can be built, that is very easy to use, cheap in cost and also has different usability like- portable functionality, no internet access, optimized local LAN bandwidth, Audio &Video calling, Web conferences, Document uploading & sharing, Email, Fax, communicating through windows phone or android smart phones and many more [1]. The system is also referred as a private branch exchange that composed with public switched telephone network. But in case of circuit switched network most of the times needs big areas, excess equipment's and other circuitry materials [2]. The system consists of one or more SIP phones, VoIP phones, PBX server and optionally includes a Gateway. SIP clients can be either soft phones or hardware based phones. The first process is to register with the server and when anyone wish to make a call one have to ask the system to establish the connection [3]. The server has a directory of all phones or users and their corresponding SIP addresses. Users of the system share a number of lines for making external or internal phone calls.

This system can be implemented and integrated with all possible feature, like –

- Supplementary VoIP protocols,
- Voice call integration
- Video call integration
- Audio & Video conferencing
- Web base conference
- Instant messaging (chat)
- Unified messaging
- Voice mail integration
- E-mail (postfix) integration
- Fax
- Mobility features (including extension mobility)
- Application & Document sharing
- Desktop sharing
- File transfer

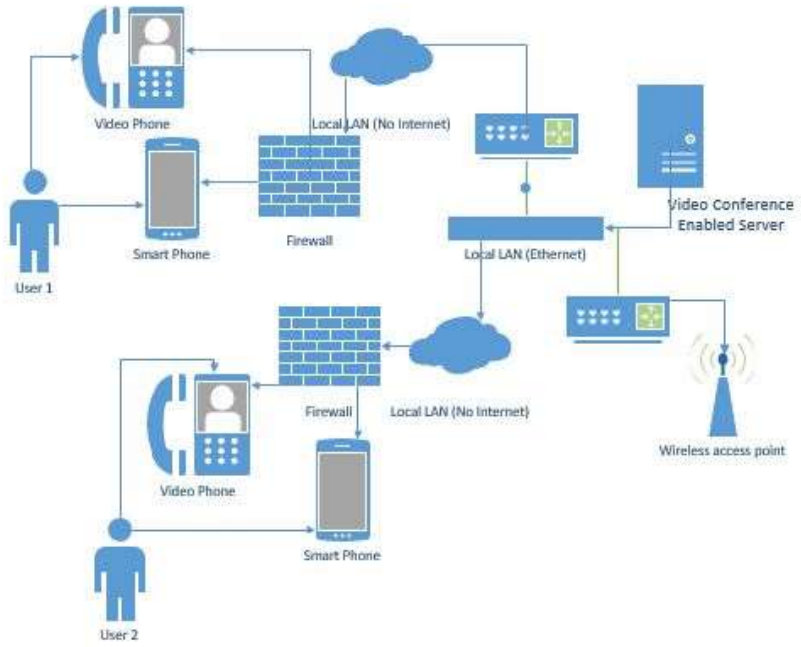

Figure 1: Overview of the System

2. EXISTING SYSTEM REVIEW

- Skype: It requires all time strong internet connection, if not then it makes connection delay. Video streaming requires a large amount of internet bandwidth (the capacity of the internet connection), so if your bandwidth is low, your video stream might be choppy or slow. Too many program can slow it down. It is costly to call over land line or cell phone. Call quality from Skype may suffer if you have a slower-than-average Internet connection. Customers may also experience interference during calls if using a Skype.
- Yahoo messenger: Must need a yahoo account. It has limitation in SMS service. It is not eligible for chatting. No customer service [6]. There is a lack of support for other IM clients as it cannot integrate with similar services such as AIM or Windows Live Messenger which can harm this program. Lack of Email Support.
- Gtalk: Need strong internet connection. It makes browser slower.
- MSN Messenger: It can be disrupted often. It has many problems in establishing connection. It can misinterpret a message and it might be sent to the wrong sender a lot of cyber bullying around the company could start. It can disconnect you a lot, depending on your internet connection, Webcam be a struggle getting connected to it. Cyber bullying happens a lot when MSN is used, and words can be misinterpreted. Also some features may not be compatible with different computers.

Comparisons between these systems are given bellow:

DOI : 10.31695/IJERAT.2019.3389

Table 1: Existing System Comparisons

Properties	Skype	Yahoo messenger	Gtalk
Admin defined extensions	No	NO	NO
Supplementary protocols	NO	NO	NO
E-mail (postfix) integration	YES	YES	NO
Transferring between two calls	YES	YES	YES
Voice mail integration	YES	YES	YES
Video conference calling	YES	YES	YES
Conference Video chat	YES	NO	NO
Low Cost Net Connection	NO	NO	NO
Low Bandwidth	NO	NO	NO
Web Base Interface	NO	NO	NO

3. OVERVIEW OF PORTABLE SYSTEM

Portability is an attribute characteristic to a computer program that can be used in an operating system other than the one in which it was created without requiring major changes [4]. Porting is the task of doing any work necessary to make the computer program run in a new environment. Portability has usually meant some work when moving an application program to another operating system [5]. When USB flash drive, portable hard drive or other portable device is plugged in the drive is synced and then it accesses to the software and personal data, when the device is unplugged, none of the personal data's is left behind. But proposed system has the benefit of being run on any operating system [7]. This Portable system has numerous usability like-

- A portable server works from any device (USB flash drive, portable hard drive, cloud drive, iPod, etc.)
- A portable server works as you move computers and your drive letter changes
- A portable server is self-contained in a single directory with sub-directories and files within
- A portable server doesn't leave files or folders behind except those automatically generated by Windows [8].
- A portable server doesn't leave registry entries behind except those automatically generated by Windows
- A portable server is optimized for use on removable drives.
- A portable server doesn't require additional software on the PC
- A portable server doesn't interfere with software installed on the PC

Why Portable server-

- Easier Backups
- Easy Platform Install
- Upgrade and Integration
- Self-Contained
- "No Code" Portablization
- Open Standardized Format

Making the server portable, it ensures an easy flexibility throughout the system.

3.1 Steps

- Use USB flash drive and click on run icon

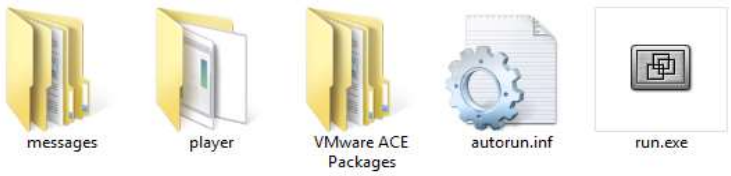

Figure 2: Click on Run Icon

DOI : 10.31695/IJERAT.2019.3389

- Then the portable server open

Figure 3: Login Area of the server

3.2 Activity Diagram of the System

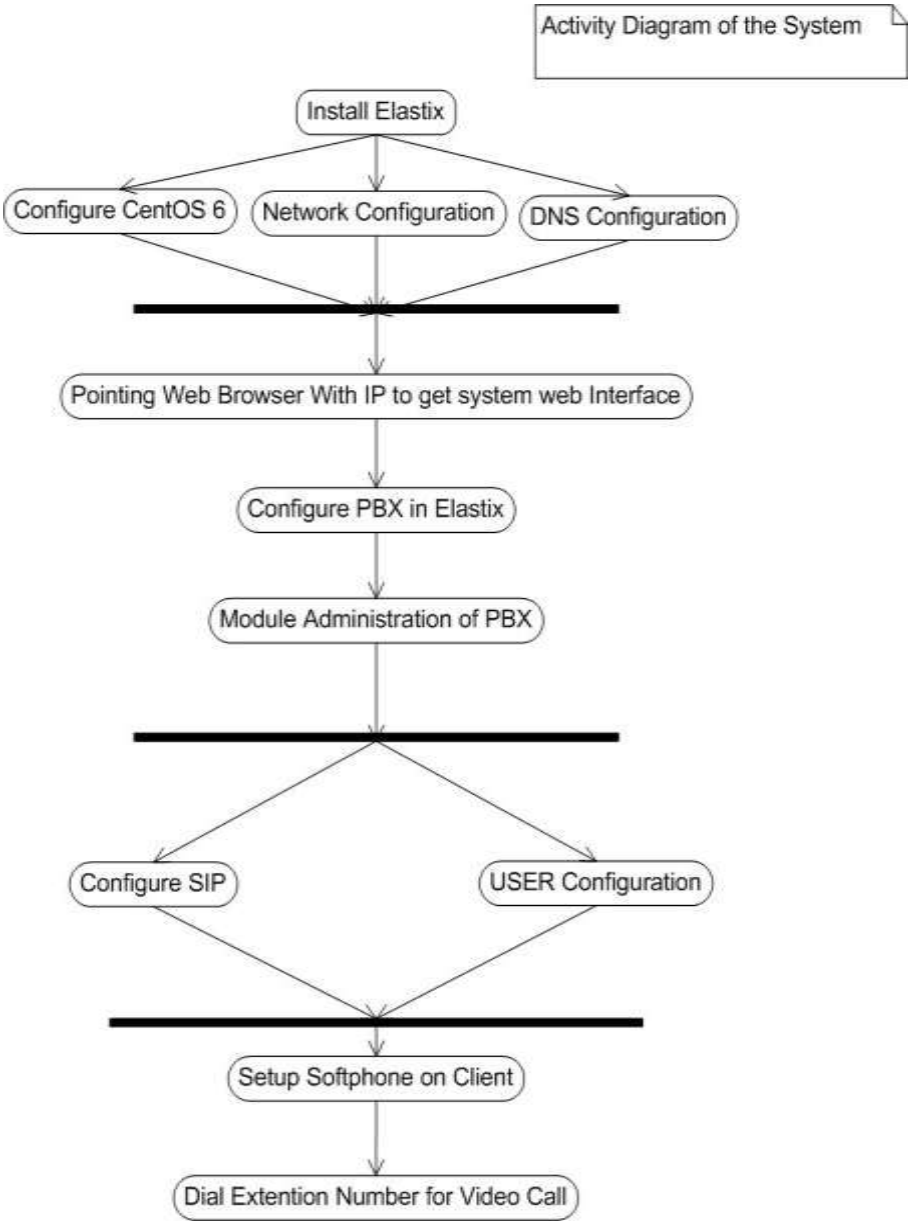

Figure 4: Activity Diagram of the System

DOI : 10.31695/IJERAT.2019.3389

3.3 Case Study

Video calls can be much easier with this system. Here admin defined extensions make interruption of unauthorized access. Configuring the extensions and the SIP credentials respectively both on server and softphones video call can be established between parties.

Example-- if IIT and other department at Jahangirnagar University one teacher of IIT wants to meet to the teacher of CSE. But he/she does not able to meet physically, then he/she can meet him/her describing his/her physical unfitness and other causes through the use of this secured Portable PABX system that is connected with this local area network (Fiber Optic Cable) without using any internet connection. By doing this he/she can also add with him/her in the video conference system that is constructed in this secured Portable PABX system.

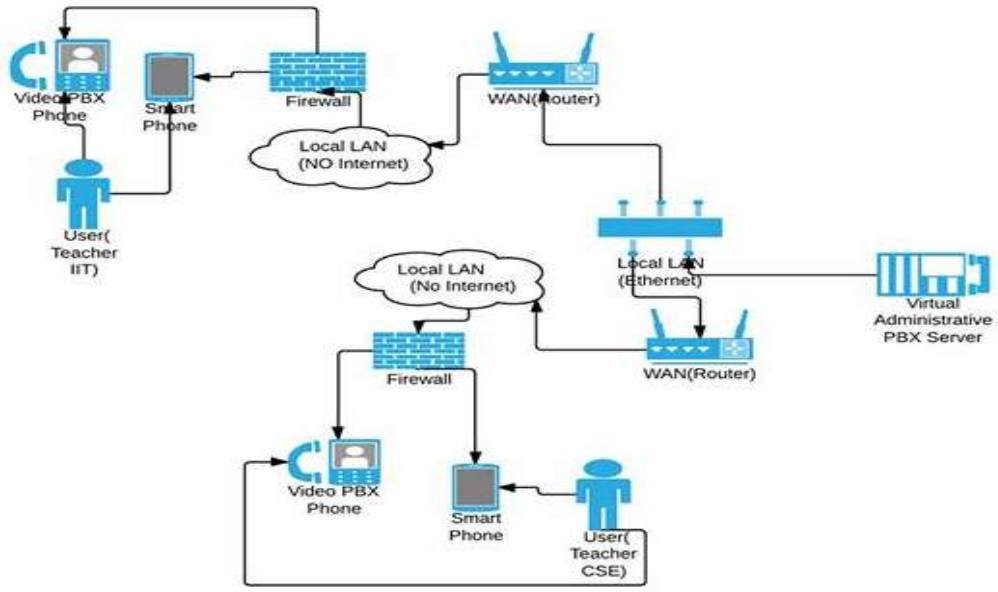

Figure 5: Communicating video call through PBX system

3.4 Video Support in the System

Go to the softphone (zoiper) and enter the called extension number and make video call

Figure 6: Caller interface

DOI : 10.31695/IJERAT.2019.3389

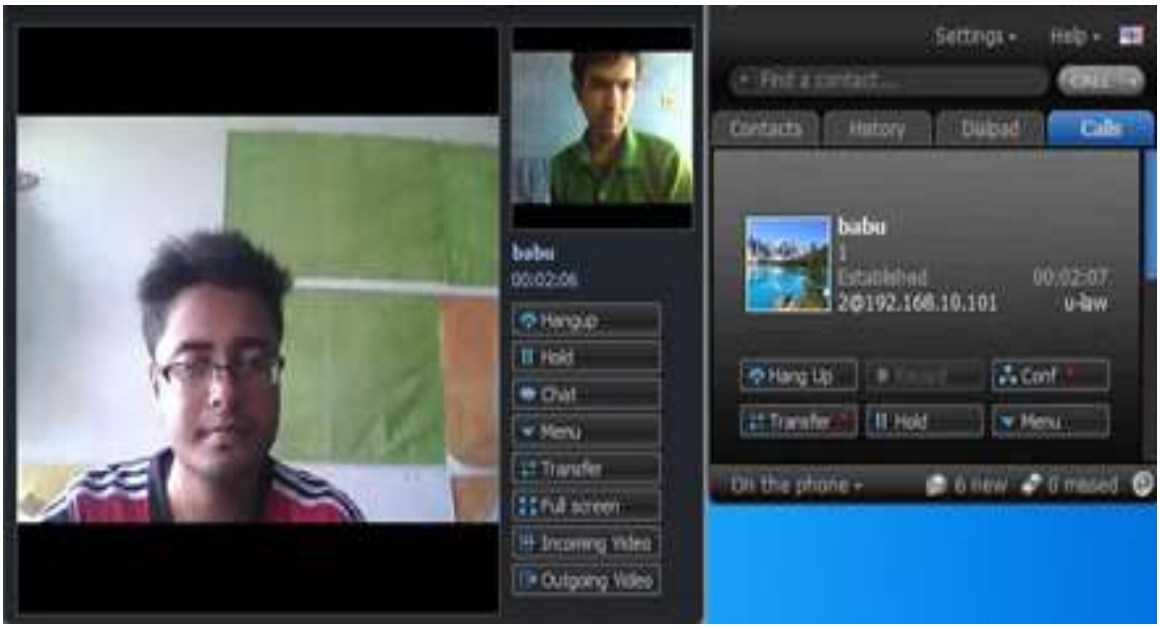

Figure 7: Called interface

3.5 Web Conference Module

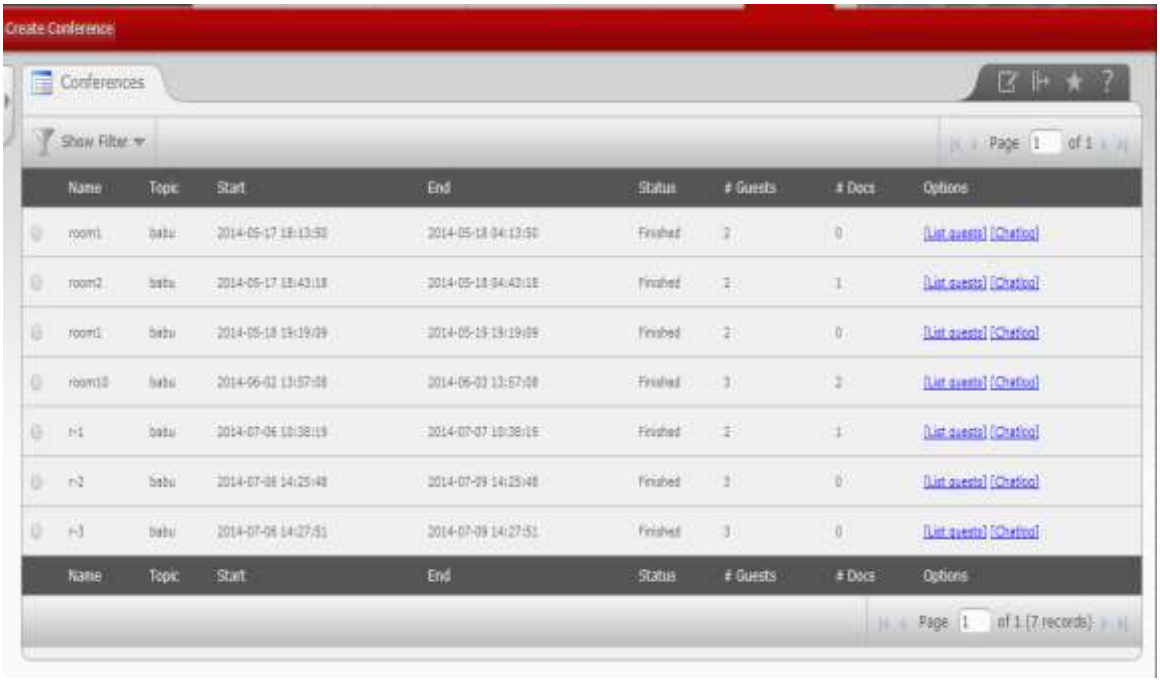

Figure 8: Web Conference Module

DOI : 10.31695/IJERAT.2019.3389

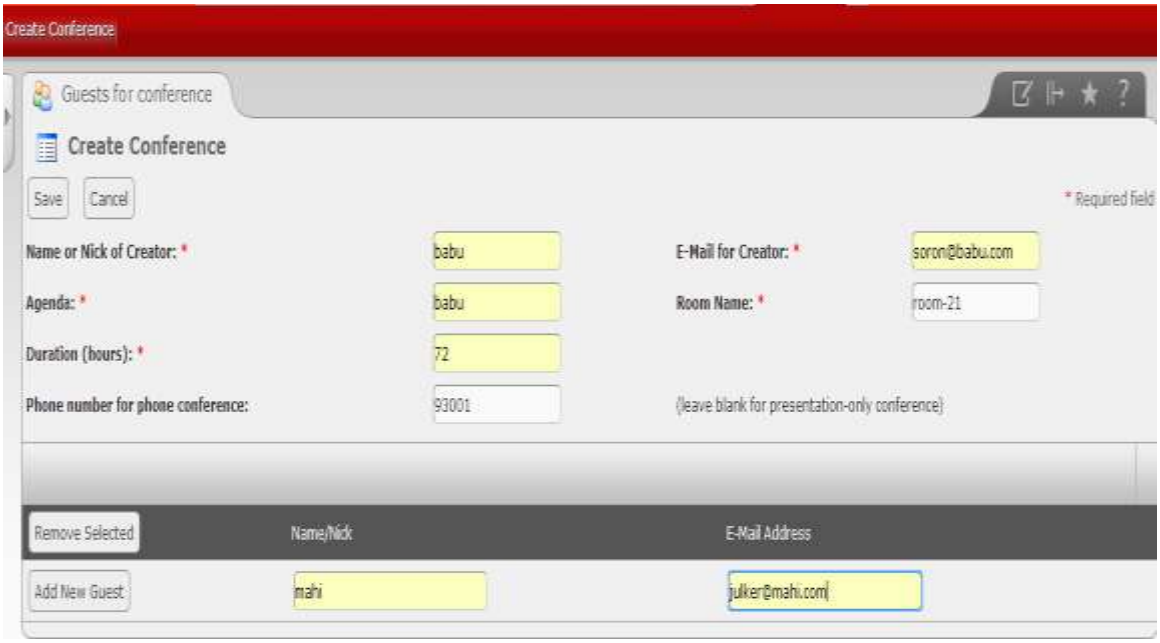

Figure 9: Create Conference

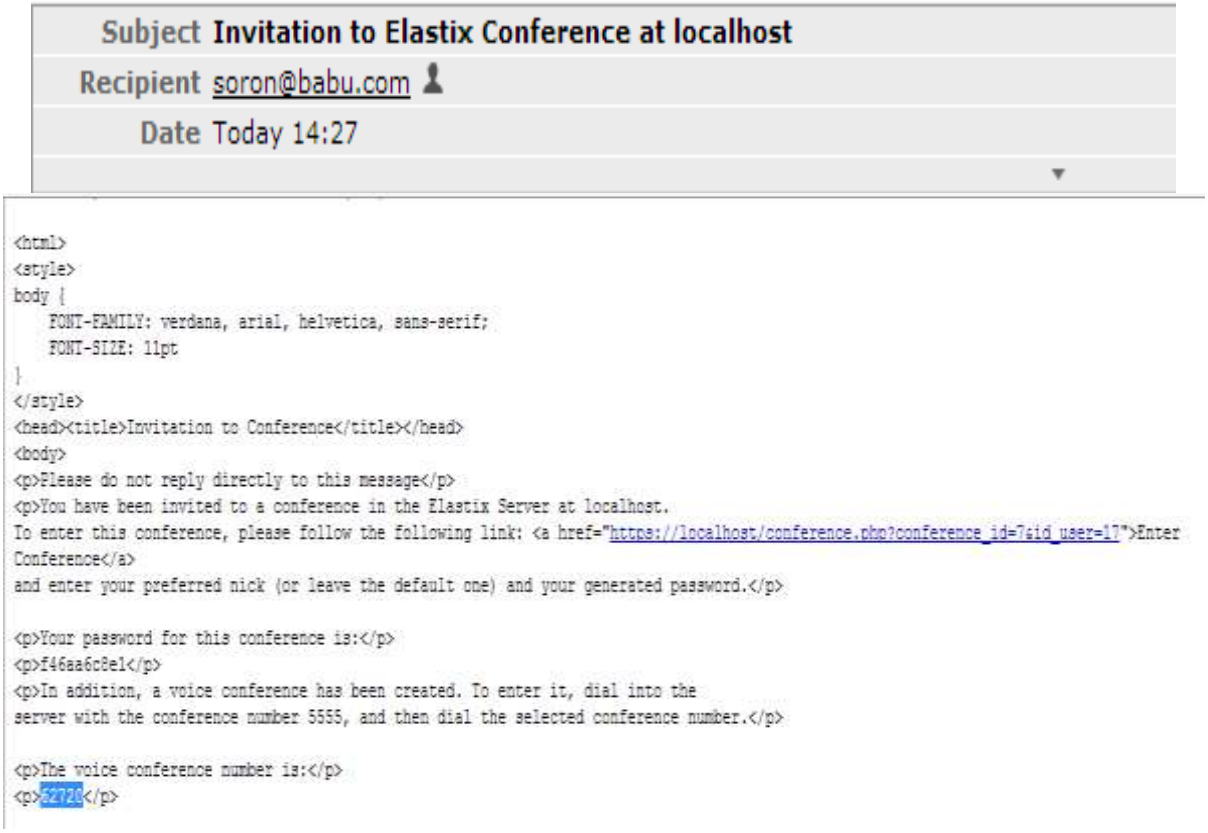

Figure 10: Invitation to conference

After clicking the conference link, the following login prompt will be displayed

DOI : 10.31695/IJERAT.2019.3389

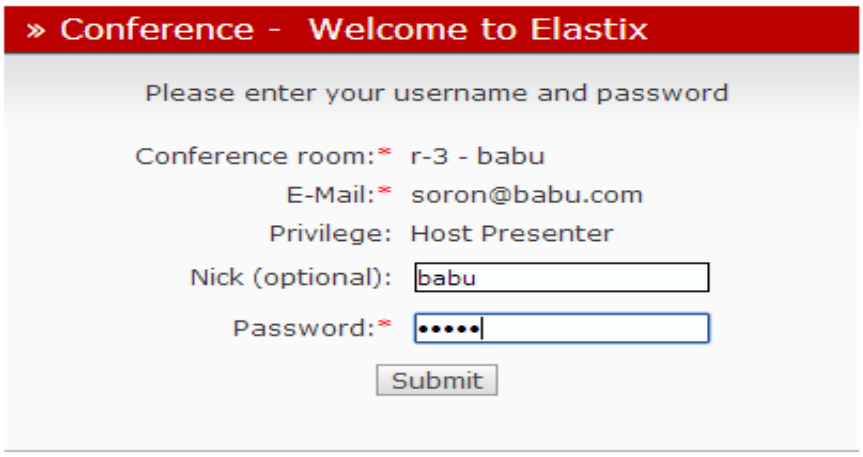

Figure 11: Login Page for Accessing a Conference

Once logged in, a screen similar to the following will be displayed

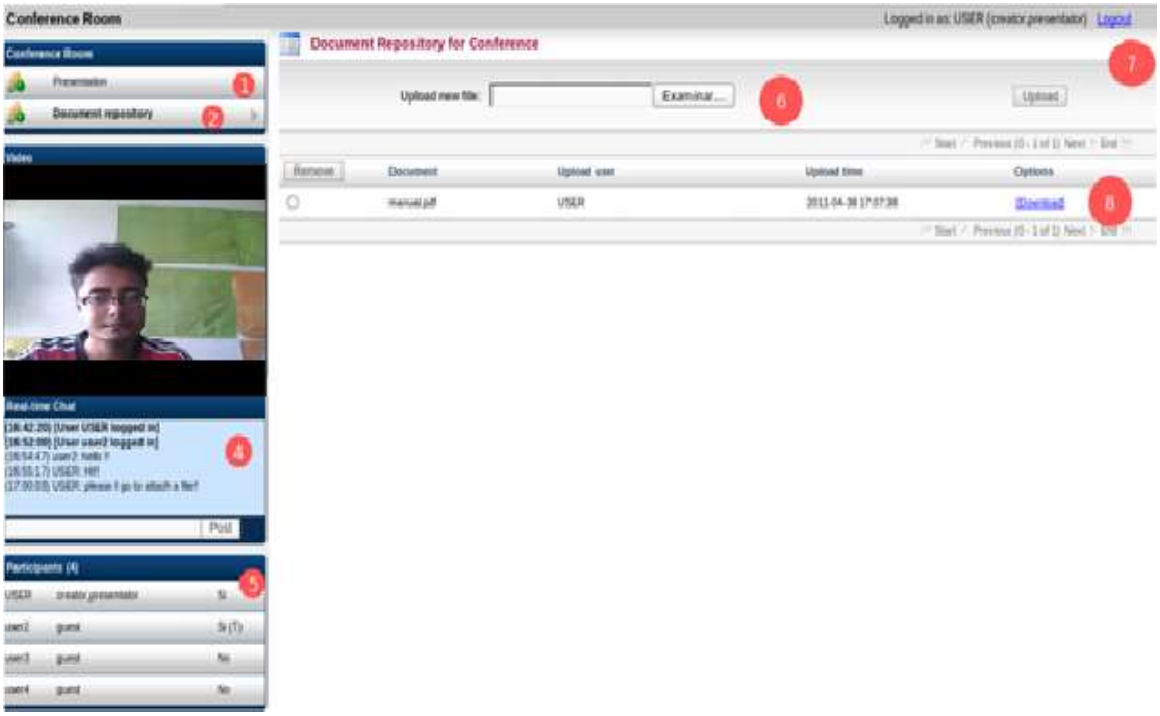

Figure 12: Accessing a Conference

- Displays the current screen.
- Shows the presentation documents that users can download.
- Video section. Displays the video from any selected participant.
- Chat panel.
- List of the conference participants.
- Section to upload files for the presentation, supports every open office file type.
- Logout link.
- List of documents used in the presentation, they can be downloaded from here.

DOI : 10.31695/IJERAT.2019.3389

4. SECURITY GOALS

To secure the system in the network, a security protocol must satisfy the following attributes: confidentiality, integrity, availability, authenticity.

- **Confidentiality** ensures that classified information in the network is never disclosed to unauthorized entities. Sensitive information, such as strategic military decisions or location information requires confidentiality. Leakage of such information to enemies could have devastating consequences.
- **Integrity** guarantees that a message being transferred between nodes is never altered or corrupted. Data can be altered either intentionally by malicious nodes in the network or accidentally because of benign failures, such as radio propagation impairment or through hardware glitches in the network.
- **Availability** implies that the requested services (e.g. bandwidth and connectivity) are available in a timely manner even though there is a potential problem in the system [9]. Availability of a network can be tempered for example by dropping off packets and by resource depletion attacks.
- **Authenticity** is a network service to determine a user's identity. Without authentication, an attacker can impersonate any node, and in this way, one by one node, it can gain control over the entire network.

Finally, non-repudiation ensures that the information originator cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes.

4.1 Security Attacks

- **Passive attacks**: A passive attack does not disrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated. Detection of passive attack is very difficult since the operation of the network itself doesn't get affected. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted, thereby making it impossible for the attacker to get useful information from the data overheard.
- **Active attacks**: An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks can be internal or external. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation (masquerading or spoofing), modification, fabrication and replication.
- **Man-in-the-Middle Attack**: In this attack, a malicious node impersonates the receiver with respect to the sender, and the sender with respect to the receiver, without having either of them realize that they have been attacked with an intension to read or modify the messages between two parties.
- **Information disclosure Attack**: In this, a compromised node may leak confidential information to unauthorized nodes in the network. Such information may include information regarding the network topology, geographic location of nodes or, optimal routes to unauthorized nodes in the network. Attacks such as location disclosure and traffic analysis come under this category.
- **Attacks using Modification:** This attack disrupts the routing function by having the attacker illegally modifying the content of the messages. Examples of such attacks include redirection by changing the route sequence number and redirection with modified hop count. Some of the attacks involving packet modification are given below:

Misrouting Attack: In the misrouting attack, a non-legitimate node redirects the routing message and sends data packet to the wrong destination. This type of attack is carried out by modifying the final destination address of the data packet or by forwarding a data packet to the wrong next hop in the route to the destination.

Denial of service (DoS) attack*:* In this type of attack, an attacker attempts to prevent legitimate and authorized users of services offered by the network from accessing those services. A DoS attack can be carried out in many ways and against any layer in the network protocol stack. The classic way is to flood packets to any centralized resource used in the network by modifying the routes information in the packets so that the resource is no longer available to nodes in the network, resulting the network no longer operating in the manner it was designed to operate. This may lead to failure in the delivery of guaranteed services to the end users.

4.2 Security Mechanisms and Solutions

Having seen the various kinds of attacks possible on the system, we now look at various techniques employed to overcome these attacks. There can be two types of security mechanisms: preventive and detective. Preventive mechanisms are typically based on message encryption techniques, while detective mechanisms include the application of digital signature and cryptographic hash functions.

DOI : 10.31695/IJERAT.2019.3389

Message Encryption: Message encryption is the technique of transforming a message into a disguised message which no unauthenticated individual can read, but which can be restored in its genuine form by an intended receiver. The plaintext is converted into cipher text by the process of encryption, which can be done by the use of certain algorithms or functions. The reverse process is termed as decryption. The process of encryption and decryption are governed by keys, which are small amount of information used by the cryptographic algorithms [10]. There are two types of encryption techniques: symmetric key and asymmetric key (or public key). Symmetric key cryptosystem uses the same key (the secret key) for encryption and decryption of a message, whereas asymmetric key cryptosystems use one key (the public key) to encrypt a message and another key (the private key) to decrypt it. Public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used for decryption purpose. Even if attacker comprises a public key, it is virtually impossible to deduce the private key. Symmetric key algorithms are usually faster to execute electronically than the asymmetric key algorithms.

Asymmetric key algorithm is comparatively slower process than symmetric but could be a great use in the establishment of a secure network system. Here I use the asymmetric-key cryptography for my proposed network.

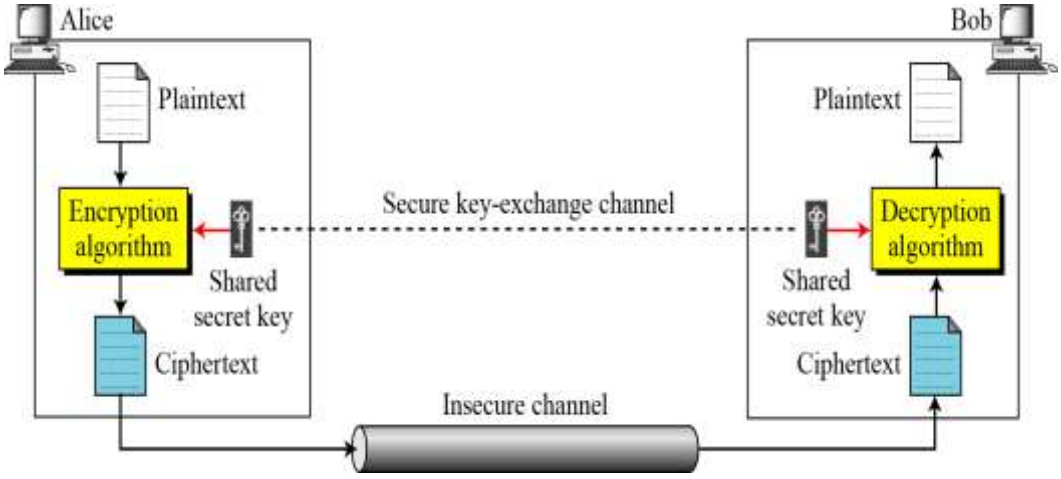

Figure 13: General idea of symmetric-key cryptosystem

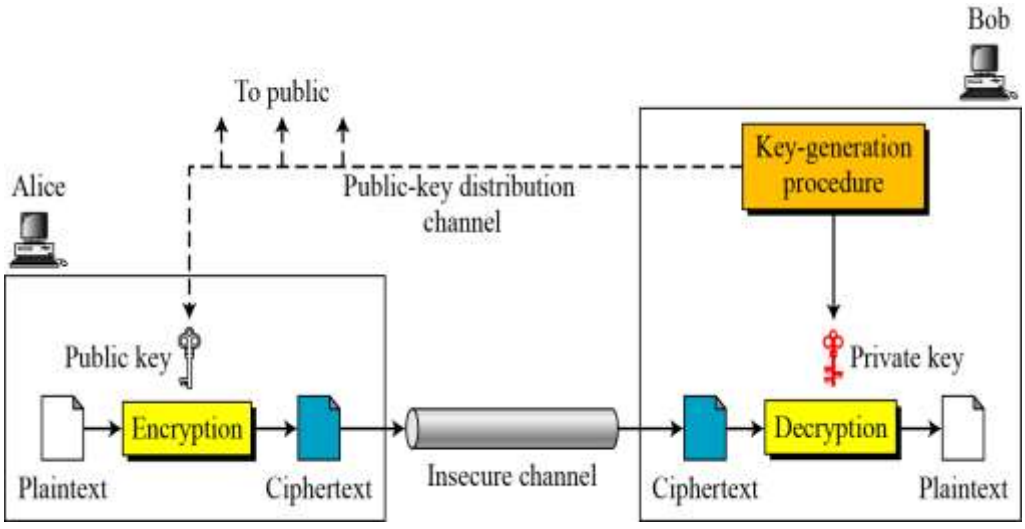

Figure 14: General idea of asymmetric-key cryptosystem

Digital signature and Hashing: The process of encryption only ensures the confidentiality of the message being sent. Digital signature is a technique by which one can achieve the other security goals like message integrity, authentication and non-repudiation. In digital signature, a block of data or a sample of the message (called a message digest) represents a private key. When this message digest is encrypted with the owner's private key, then a digital signature is created. This digital signature is then added at the end of each message that is to be sent to the recipient [11]. The recipient decrypts the message using the owner's public key and thus verifies that the message digest is correct and the message has come from the genuine sender. The process of digital signature is outlined below:

DOI : 10.31695/IJERAT.2019.3389

- Sender generates a message.
- Sender creates a "digest" of the message.
- Sender encrypts the message digest with his/her private key for authentication. This encrypted message digest is called digital signature.
- Sender attaches the digital signature to the end of the message that is to be sent.
- Sender encrypts both the message and signature with the recipient's public key.
- The recipient decrypts the entire message with his/her private key.
- Thus, the recipient verifies the digest for accuracy.

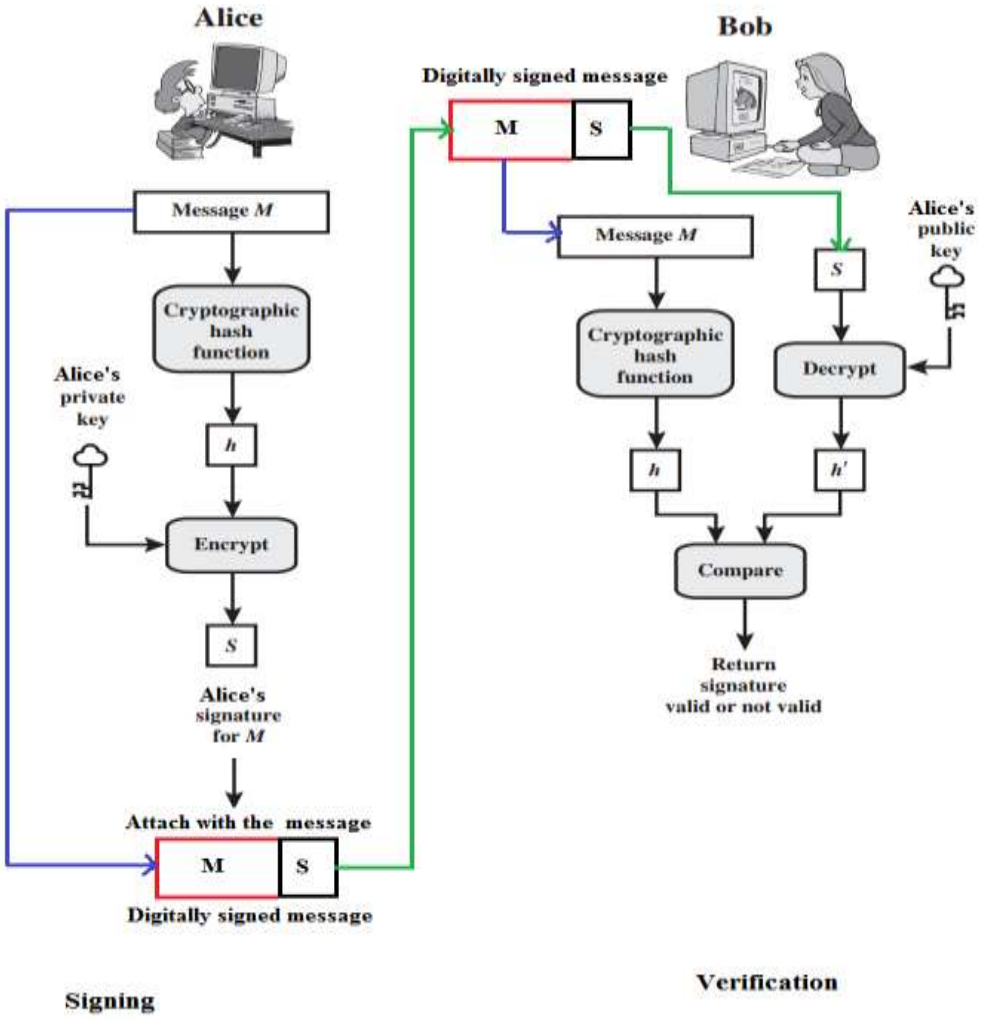

Figure 15: Illustration of digital signature process

Hashing can be used for the digital signature process especially when the message is long [12]. In this the message is passed through an algorithm called cryptographic hash function or one-way hash function before signing [13]. Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. A hash value (or simply hash), also called a message digest, is a number generated from a string of text. The hash is substantially smaller than the text itself. In hashing, a fixed-length message digest is created out of a variable-length message. The digest is normally much smaller than the message. It plays a vital role in security system that creates a unique, fixed-length signature for a message or data set. People commonly use them to compare sets of data [14]. Since a hash is unique to a specific message, even minor changes to that message result in a dramatically different hash. Therefore, it is very resistant to tampering.

DOI : 10.31695/IJERAT.2019.3389

4.3 Flowchart of overall Security Mechanisms

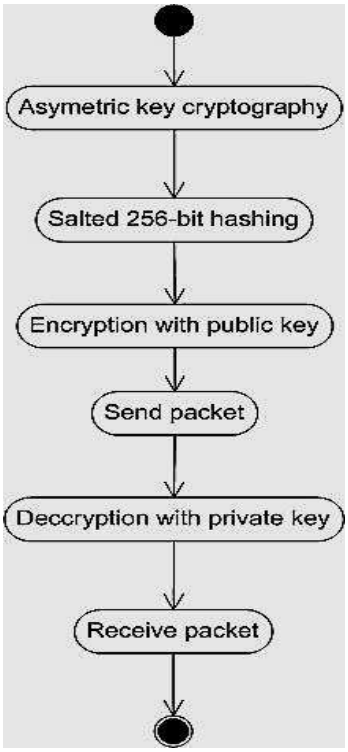

Figure 16: Flowchart of overall Security Mechanisms

5. FUTURE WORKS

Theoretical and applied research can be performed for reaching higher optimization. In future, this system can be integrated with real time server and also can be incorporated with other domain like education, finance & business sectors. The third-party services like map, GPS can be included in the system which work with low internet speed. This system can be implemented with cloud based platform which is more flexible to have all or part of our Unified Communication in the cloud, lower cost of ownership, simple and easy to budget for, empower mobile staff, improve collaboration and strengthen relationships through optional multi-party video meetings, secure access from more places. This system can be increasingly sophisticated, particularly with the emergence of WebRTC, which is a game changer for Unified Communications, offering simpler and cheaper real-time communications options and brings all of the plusses of enterprise video-multi-tasking and collaboration, less travel for in-person meetings without the costly infrastructure and human resources investment. Wireless sensor network in the business organization can be made with the help of this system. Moreover, this system should be more accurate with proper security mechanism.

6. CONCLUSION

This is a unified communicative portable system that can mark a new dimension in the mobility management as well as other networking solutions. It can be the most cost reduced communication system with limited utilities that works with better administrative options. Its user-friendly environment and portability technology can be mounted to anywhere. The Proposed system can create complete modern hassle-free communication environment with platform free equipment's. The system can play a vital role to design a secured portable optimized platform that works on any platform anywhere. Thinking to make the system a small package but bigger in work form so that one can work with limited equipment's and it has better security and administrative options. The unified communicative portable system can give people of all aspects a ready-made unified communication platform that is hardware and software independent.

REFERENCES

[1] Li, Chong, et al.,"A High Efficient Unified Communications System Based on Elastix", Microcomputer Applications 7 (2011): 006.

[2] Luksa, Darko, Sinisa Fajt, and Miljenko Krhen,"Sound quality assess-ment in VOIP environment", Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on. IEEE, 2014.

[3] Gough, Michael,"Video Conferencing over IP: Configure, Secure, and Troubleshoot: Configure, Secure, and Troubleshoot", Elsevier, 2006.

DOI : 10.31695/IJERAT.2019.3389

[4] Campbell, Robert Craig, et al.,"Videophone and method for a video call", U.S. Patent No. 7,404,001. 22 Jul. 2008.
[5] Hakusui, Shigeaki,"Virtual PBX based on feature server modules", U.S. Patent No. 8,279,857. 2 Oct. 2012.
[6] Berry, Alfred E., et al.,"Integrated audio and video agent system in an automatic call distribution environment", U.S. Patent No. 6,404,747. 11 Jun. 2002.
[7] Ajasa, A. A. A., and O. Shoewu. "Exploiting VoIP Telephony in IP-Pbx Solution."
[8] Md.Torikur Rahman, Md.Julkar Nayeen Mahi, Milon Biswas, M.Shamim Kaiser and Shamim Al Mamun, "Performance Evaluation of a Portable PABX System through Developing New Bandwidth Optimization Technique", 2nd International Conference on Electrical Engineering and Information & Communication Technology(ICEEICT 2015), IEEE.
[9] Androulidakis, Iosif I.,"PBX Security and Forensics: A Practical Ap-proach", Springer Science and Business Media, 2012.
[10] Behrouz A. Forouzan,"Cryptography and Network Security" Special Indian Edition, Tata McHill publication, 2007.
[11] Kaufman, Charlie and Perlman, Radia and Speciner, Mike,"Network security: private communication in a public world" Prentice Hall Press, 2002.
[12] Phithakkitnukoon, Santi, Ram Dantu, and Enkh-Amgalan Baatarjav. "VoIP Security—Attacks and Solutions." Information Security Jthisnal: A Global Perspective 17, no. 3 (2008): 114-123.
[13] Md.Torikur Rahman and Md.Julkar Nayeen Mahi, "Proposal for SZRP Protocol with the Establish-ment of the Salted SHA-256 Bit HMAC PBKDF2 Advance Security System in a MANET", 1st Interna-tional Conference on Electrical Engineering and Information & Communication Technology(ICEEICT 2014), IEEE.
[14] Md.Torikur Rahman, "Enhancement of Inter-Vehicular Communication through a New Bandwidth Optimization Technique to Optimize the Performance of VANETs", International Journal of Science and Research, Vol. 8, Issue 2, February 2019, pp. 966-971, ISSN 2319-7064.

DOI : 10.31695/IJERAT.2019.3389