Securing High Level Data Services from Different Threats: SPAM Over Internet Telephony, Eavesdropping, Denial of Service, Call Tampering

Farrukh Musa[1] **and M. Junaid Arshad**[2]
[1,2]Department of Computer Science and Engineering, University of Engineering and Technology, Lahore, Pakistan
[1]farrukhmusa@hotmail.com

Abstract— **Communication technologies use have been largely transformed with the introduction of digital and high-level data services over Internet Protocol which fuses telecommunication and digital television delivery services together. Another revolution is that the user will be capable to have a bidirectional communication, the ability to interact with the service provider and enjoy high quality end-to-end service. These high-level data services afford rich multimedia services over a measured IP network. Networks require advanced security solution that protects data from hackers, threats and vulnerabilities resulting in secure high-level data services. This research work gives an overview of these high-level data services, security problems and threats that should be resolve for better quality and greater safety. It also identifies and describes the best techniques to secure VOIP that are acceptable and effective for the call participants. As a result, with this research work user will become familiar with the security risks that must be removed while doing any conversation.**

Keywords— **High Level Data Services, Security Threats in VoIP, SPAM Over Internet Telephony, SPIT, Eavesdropping, Denial of Services and Call Tampering**

I. INTRODUCTION

Nowadays telephonic services are using everywhere in the world or in other words we can say that it has been developed to an ever-present service. People can be accessible and can make themselves in touch with others anytime, anywhere from where ever they are. Beside with it, the Internet has arisen to an imperative communication medium. These facts and the growing availability of broadband internet access have focused to the mixture of these facilities. Voice over Internet Protocol (VoIP) is the keyword that describes this mixture. The benefits of VoIP in comparison to ordinary telephony are location liberation, simplification of transport networks, ability to launch multimedia communications and the very low costs and investment [1].

In VoIP innovation domains of communication, information is incorporated, by allowing the transmission of voice content over the Internet, an intranet and other new/old system utilizing bundle exchanging innovation. VoIP benefit that utilized a few methods has many focal points, for example, multimedia, a voice administration, and extra administration with minimal effort [2].

Be that as it may, the different tricks rise utilizing VoIP in light of the fact that VoIP has the present vulnerabilities at the Internet and grounded on complex advancements which include protocols, interfaces and diverse segments, conventions. VoIP web foundation is utilized for voice interchanges. Information bundles pass on voice motions as general internet movement. More than the PSTN network, this plan is further more proficient and productive. One noteworthy utilization for companies in changing from a customary communication framework to VoIP is costly, VoIP foundation.

All things considered, one can without much of a stretch see, these advances dependably raise new issues and difficulties that must be engaged and comprehended. Nowadays, it is obvious that spamming is the most aggravating actuality of the Internet. Diverse sources illuminate that email spam is measured to be 80 to 90 percent delivered of the email traffic. Security experts guarantee that these will victory on VoIP too. Spam over Internet Telephony (SPIT) or Voice spam dangers is significantly more genuine when contrasted with the dangers that gets up from email spam, for the unsettling influence and irritation perspective is considerably more prominent [3], [4]. The capability of SPIT has diminished the efficiency of email spam; as result each SPIT call quickly intrudes on the call by the ringing telephone. An email that hits the inbox at a young hour is pointless yet won't irritate the client much, conversely a ringing telephone around then will prompt a substantially higher unsettling influence. Each media transmission systems, including VoIP, have issue of dangers and assaults. These incorporate alteration, block attempt, and even an information can be misfortune amid this. SIP protocol is specifically extremely powerless to adjustment, redirection, or end of the calls. In addition, in IP communication, it isn't conceivable to arrange singular parcels to front and examine them by return in light of the fact that the correspondence occurs continuously [5]. This is the principle distinction between the proposed security instruments for established Internet administrations and VoIP.

In this research work we describe the security threats and issues in application with data services mainly we refer to VoIP, that are nowadays increasing day by day with the passage of time. We will discuss some main issues that cause different abnormalities to the system which includes spamming, eavesdropping, denial of service threats, call tampering that harms the system as well as the user. Major risks are highlighted that must be in consideration while using such data services and to let you know how different people, strangers are misusing your confidential data and misleading your messages. This will help the participants to make their conversation safe and secure form such threats.

II. LITERATURE REVIEW

The beginning of VoIP appropriation was described by an absence of concern and mindfulness about security issues identified with its utilization. To be sure, serving organizations and clients were for the most part engrossed with issues identified with its quality, usefulness, and cost. Since VoIP is a standard technology of communication, security has turned into a noteworthy issue.

A fundamental shortcoming of VoIP communication is surely the frequently low quality of voice, which brings about consistent resound or static clamors. A further blind side is the whole reliance on the individual broadband Internet association, which altogether decides the voice nature of the VoIP call [6,7]. Since VoIP works through the broadband Internet association, it doesn't have an inward power cable the way a typical phone line does. What's more, crisis telephone gets can't be completed adequately since they can't be followed back by administrators.

Kim et al (2008), TLS and S/MIME are proposed for SIP flagging message assurance and SRTP for media insurance. MIKEY is likewise a standard convention for key administration. In this research, they find out and executed security conventions for VoIP [8]. And afterward, they fulfilled execution trial to assured the quality of them by applying actualized security protocols to equipment VoIP telephone and SIP proxy.

The productiveness of all VoIP spam preventive methods would raise positive value ratio for its security. Measuring viability is likewise a subject that requirements additionally study about, with respect to most explained strategies no genuine test information is accessible in regards to their adequacy [9].

Thirunavukkarasu et al (2015) expresses an agreeable relay network comprising of a source, a goal, and different decode and forward (DF) relays within the sight of numerous eavesdroppers, which expect to tap private messages transmitted by both the source and the relay. For purported secrecy maximization oriented relay selection (SMORS) conspire is acquainted with enhance the physical-layer security of remote correspondences. In the SMORS conspire, a relay with the maximal mystery rate is chosen among all the DF relays to forward the source flag [10].

In a helpful system with various relays within the sight of numerous eavesdroppers, SMORS plot is proposed to enhance the physical-layer security of remote correspondences. In the SMORS plot, the relay with the most extreme prompt mystery rate is chosen among all DF relays to forward signs got from the source to its goal.

Q. Yan et all (2015) represents that the DDoS threat is a kind of cyber threat that uses expansive quantities of PCs and enormous volumes of movement to overpower a server or system, abating it or rendering it totally insensitive. DDoS threats for the most part require that the aggressor control thousands, several thousand or a huge number of PCs – typically claimed by ordinary, clueless buyers everywhere throughout the world – and make their own system out of these "zombie computers" [11]. That huge network of systems is then used to center movement, for example, a straightforward demand to see a website page or something more malicious, on a solitary target or gathering of targets. The focused on servers or systems, not intended to deal with synchronous solicitations from such vast quantities of networks, regularly get hindered or quit reacting totally. The measure of movement created by these threats is immense.

Mobile phones are defenseless against threat by malware, worms, and other system infections. These infections commandeer PC frameworks and take control [12]. They can send spam and different malicious information, target and for all time disturbed data, and follow keystrokes and information passage to empower remote access. Visa information and money related data are especially defenseless in this kind of threat [13].

In the current era, the best protection shield is a decent offense, and this remains constant with VoIP security [14]. Smart organizations can preemptively shield themselves from these strategies for potential threats utilizing different methods describes as follows:

- ***Encryption:*** Cloud correspondence suppliers offer client rules for encryption and confirmation conventions, and many offer encryption as an extra service. While all organizations should work to guarantee extreme client security, financial services, those inside retail and different businesses managing customer information must take additional measures.
- ***Authentication Protocols:*** VoIP authentication protocols differ in light of the kind of information being transported. They extend from a normal secret key validation technique to an intricate three-way confirmation process that ensures servers and business VoIP. Secret key verification, likewise called the two-way handshake, is exceptionally powerless against

threats and is effortlessly abused by programmers. Ordinarily, the username and secret key are not adequately masked or encoded before navigating the connection. Using a VPN or a safe MPLS arrange instead of the open Internet can lessen this hazard essentially.

- ***Challenge-Handshake Authentication Protocol (CHAP):*** At the point when the calling customer (PC or mobile phone that sends information and instates a VoIP call) joins with the application administrator situated in the VoIP server, the authentic one utilizes a three-advance procedure to decide authenticity. Additionally, called a three-way handshake, CHAP concedes or denies get to. On the off chance that the scrambled messages don't coordinate after the test and reaction steps, the customer gets a disappointment message and is denied access to the VoIP framework. This counteracts fake VoIP calling.
- ***Antivirus Software:*** Since VoIP mobile phones are a piece of system networks, shielding them from corrupt files and different risky outsider projects is seriously risky. Viruses comes in an association's VoIP network through email to trade off existing security conventions and hinder or suspend VoIP organize benefits altogether. Introducing and keeping up antivirus and against malware programming programs like firewalls is critical. Regularly, VoIP merchants or system suppliers offer antivirus insurance, otherwise called bound together danger administration programming, as a major aspect of their administration services.

Looking to the Future

System security attacks are always developing and leads to huge risk so on other hand the protecting measures must progress correspondingly. Protecting restrictive business or organization's data and delicate client information definitely secure and confidential at all levels. Client, representative, and interior records information stay top focuses of cyber threats, and the harm to organizations reputation as revealed. Organizations must be watchful keeping in mind the end goal to maintain a strategic distance from exorbitant and badly designed security attacks.

As the telecommunication business advances to a progressively computerized stage, new sorts of cyber-attack dangers will keep on targeting information, applications, and systems. Cooperating with the correct security administrations supplier upgrades a business' capacity to check these developing system attacks.

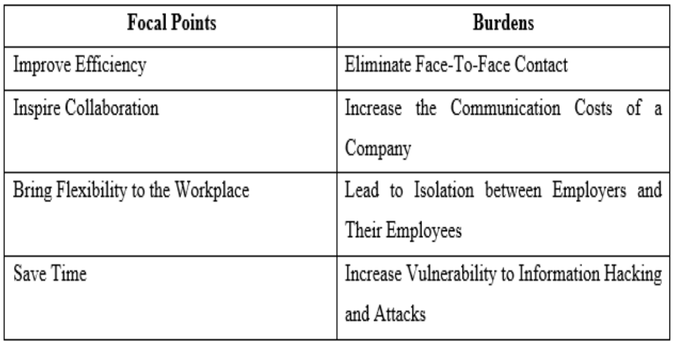
Successful accomplices empower organizations to distinguish, break down, and react to cyber-attacks before they harm their status and primary concerns. Associations can tackle the learning of these specialists and their bleeding edge tools to ensure data in this growing opposed condition.

III. RESEARCH METHODOLOGY

This examination and research is to make VoIP to secure from intruders and attackers. In above literature review, number of attacks are grow through in detail especially Spamming, Eavesdropping, Denial of Service and Call Tampering alongside their accessible results and will try to distinguish the better solutions from the one that are addressed previously. In spite of the fact that the way that VoIP is currently large number of people are engaged with VoIP but the innovation is far from create in the security world. Preventive protocol makes it hard to between interface things from different trader. VoIP cell phones are a bit of PC frameworks, protecting them from threats and distinctive perilous outcast tasks is fundamental.

Attacker enters an association's VoIP structure through email to deal existing security convention sand ruin or suspend VoIP systems benefits completely. Presenting and keeping up antivirus and threatening to malware programming programs like firewalls is crucial. Progressions in telecommunication advancements have enormously affected in a way individuals connect with each other at the worldwide. These days, people and organizations can impart effortlessly through voice calls, video calls and information sharing applications. By receiving a modern media transmission system, numerous organizations have acknowledged enhanced efficiency, better customer services and expanded development. Following are some real focal points and burdens of telecommunication shown in Table I.

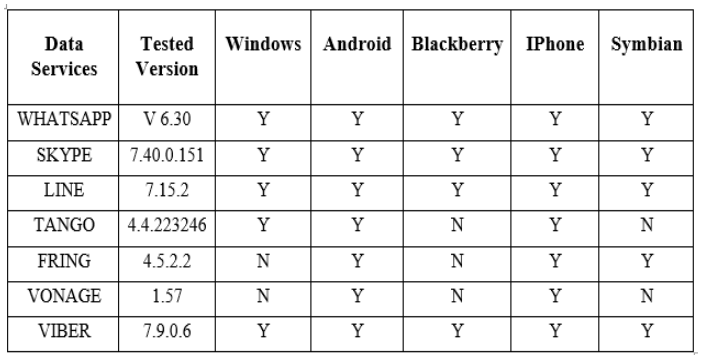
Table I: Focal Points and Burdens of Telecommunication



Focal Points	Burdens
Improve Efficiency	Eliminate Face-To-Face Contact
Inspire Collaboration	Increase the Communication Costs of a Company
Bring Flexibility to the Workplace	Lead to Isolation between Employers and Their Employees
Save Time	Increase Vulnerability to Information Hacking and Attacks

Consistently, VoIP traders or framework providers offer antivirus confirmation, generally assembled brought chance administration programming, as a noteworthy part of their administration offerings. Skype uses its own prohibitive that safe VoIP correspondence convention. The Skype server affirms the customer open keys using either 1536 or 2048-piece RSA confirmations. Since it is insignificant to choose the target's Skype ID, an attacker can along these lines talk with the goal over Skype to choose his/her IP address, paying little respect to the likelihood that the goal is behind a network address translation (NAT) server. As Skype offers end-to-end encryption, no information about the coordinating of the data parcels could be found from the stream content. Similarly, there are many other high level data services that are running all over the world on daily basis. Some commonly running applications are used for the analysis as describes in the following Table II.

Table II: High Data Services available on different platforms



Data Services	Tested Version	Windows	Android	Blackberry	IPhone	Symbian
WHATSAPP	V 6.30	Y	Y	Y	Y	Y
SKYPE	7.40.0.151	Y	Y	Y	Y	Y
LINE	7.15.2	Y	Y	Y	Y	Y
TANGO	4.4.223246	Y	Y	N	Y	N
FRING	4.5.2.2	N	Y	N	Y	Y
VONAGE	1.57	N	Y	N	Y	N
VIBER	7.9.0.6	Y	Y	Y	Y	Y

These all high level data services give the privacy at limited boundary, which mean all provides security in the form of encryption while texting but on other at the time of voice communication these services shows soft wall. Application like skype, WhatsApp, line does encrypt your voice but on darker and bigger side there is such method to secure a voice communication.

Researching and getting literature of different solutions will be made by analyzing previous techniques and method. If essential method like analytical analysis and tabular will also be adjusted to give the better solution. Different attacks move from system to system without letting know the client. They can discover a system that has bring down security settings or overcome the weakness, and embed themselves onto that network without the client regularly realizing what is going on. Many viruses and Trojan stallions, frequently known as "bots", moves along these lines. They use the Internet to discover system to taint. The client will never realize that their network has been bargained in light of the fact that the virus enters to their system silently. Following diagram describes the architecture of VoIP and attacks from different intruders during the conversation:

As shown in Fig. 1 that how the users are connected with each other while having a communication medium. Endless supply of a simple voice (analog voice) by phone, Voice Gateway initially digitized signal and squeeze the modern digital signal as standard information piece that are commonly use with a name as IP packets. They are sent over the Internet to the passage of the Voice Gateway, where the procedure is switched. Along this innovation, to make phone to phone, phone to PC, and PC to phone communication become possible. Further due to security lacks the hacker gets open invitation to interfere in others matter and have some confidential information that is sometimes very risky with the business point of view that can be clearly seen in Fig. 1.

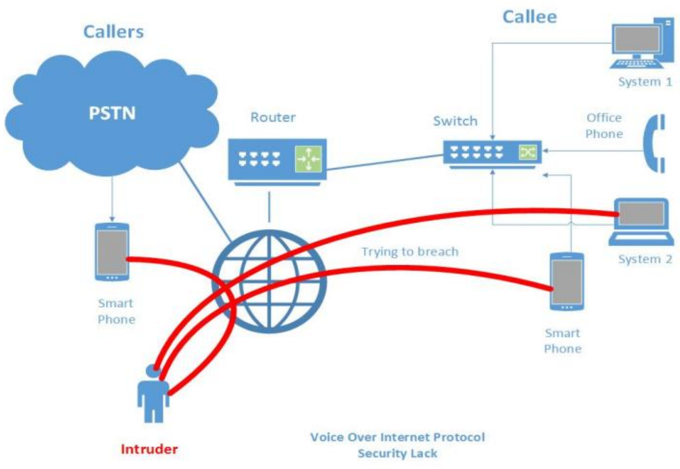


Fig. 1: VoIP Security Lack

But it can be made secure, more reliable and also can save the user from the big loss by activating the firewalls of the system.

Why to use Firewall?

Firewall is a system or you can also say it's a hardware device that shields your PC from being assaulted by intruder while using internet, worms, and viruses. This may happen either at a vast corporate system, or essentially at a network that use in home or small company; both have a similar security threats and issues. Having a firewall in each internet bundle by an organization enables the business to make online principles for the clients. As we see, with the firewall the organization can control the entrance to specific sites, giving it the control of how workers utilize the system. With the addition of Firewall between intruder and our smart phone or systems we can satisfy that our system is safe. When any intruder tries to reach the system or smart phone it can alarm us about the possible attack of the intruder. Fig. 2 show how firewall can help us in the safety of our systems and can protect our imported data from the intruders.

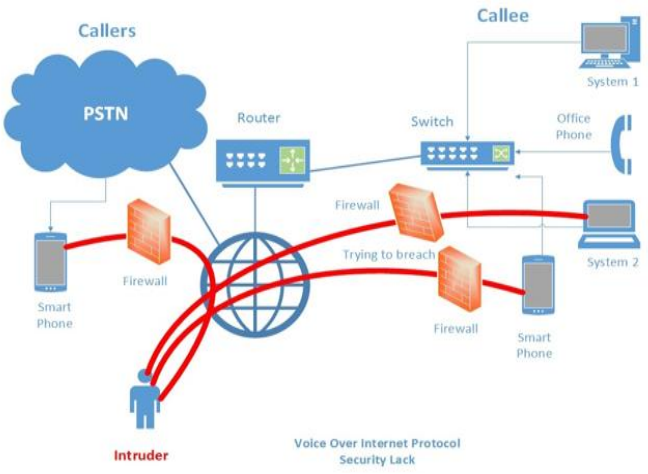


Fig. 2: VoIP Security with firewall

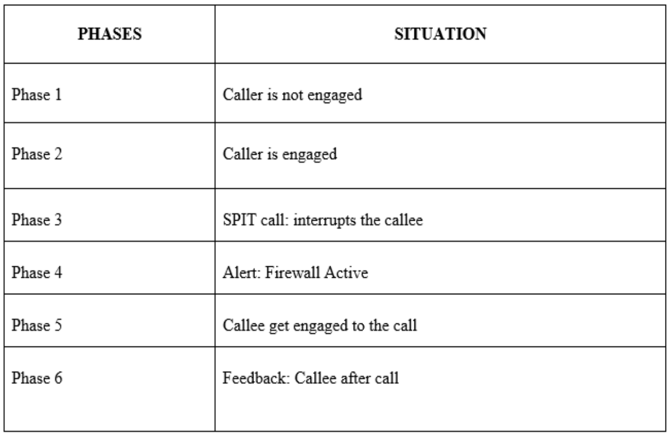
VoIP networks are basically based on difficult technologies that involves protocols, interfaces and different components due to which it is not so easy to make it secure. The different telecommunication risks can be highlighted in various ways such as services plan misuse, virus and malicious code, identify theft and many options to harm the system. So to avoid to such threats firewall can play an important role.

Firewall is really the framework which stays between your system and the worldwide system to keep shameless exercises from happening, for example, getting immaterial document that can hurt your network or system, releasing your private information and data and so on.

How to protect better along with firewall?

VoIP communication prevention system is protecting the callee from being disturbed by intruder calls, leakage, spying and any other interaction while ensuring that the callee does not miss legal calls. Preferably, this is achieved in a way which is very simple and easy to get rid of from the fake calls and illegal interaction. Based on above research, we propose a general architecture for securing VoIP communication from SPIT, Eavesdropping, Call Tampering and DoS that contains several phases as describe in Table III:

Table III: Securing call architecture



PHASES	SITUATION
Phase 1	Caller is not engaged
Phase 2	Caller is engaged
Phase 3	SPIT call: interrupts the callee
Phase 4	Alert: Firewall Active
Phase 5	Callee get engaged to the call
Phase 6	Feedback: Callee after call

Phase 1: Caller is not engaged

In phase 1 Intruder do not requires to engage with the caller, which is completely invisible to the callee. To proceed the identity of a caller is compared to the set if identities to decide whether to accept or reject the call, this is known as listing. There are two types of lists discussed as white and black. White are those which allowed to call where calls from identities and black list is to be rejected without any interaction.

Phase 2: Caller is engaged

In this section intruder requires an interaction with the caller to verify that a caller is a valid sender from the domain he is calling to the callee. Such a methodology, even if the technology is mature, is not easily applicable to real time communication and thus to SPIT prevention because of the time it takes to perform the sender check.

Phase 3: SPIT call: interrupts the callee

In this phase intruder requires an action by the callee on the arrival of a SPIT call. During the communication this phase this is the think that the caller and the callee as well do not want to face. It basically the third person that wants to get your confidential information or may want to disturbs your privacy.

Phase 4: Alert: Firewall Active

In this phase the caller gets the notification if the intruder tries to get engage with their communications. The encrypted picture code will send to the both parties and ask to tap the same image to carry on the call and on the other hand the intruder will not get the images. When the intruder will not get any image; he will automatically cut off from the call.

Phase 5: Callee get engaged to the call

At this stage both are connected with each other and are ready to communicate and share their confidential information and data.

Phase 6: Feedback: Callee after call

Now they are engaged with each other without any interference of any third party that is illegal.

IV. CONCLUSION

As the new technologies are coming into being and use of these inventions are gradually increasing day by day. Along with it the individuals are also trying intensively to misuse it in different and new ways. Nevertheless, we are getting created in all the courses in existence with most recent innovation and most recent mobiles, we can spare the time, because of that everyone can come nearer that is not common if we go few days behind, the period of mobiles had made it possible. Time is spared by utilizing most recent advancements, yet then likewise innovation is additionally having another side and which is more awful than anything as we have such huge numbers of devices and methods to distinguish the crimes however then additionally its appropriately better to remind the saying “prevention is better than cure”, thus the finest thing is to get preventive and careful than careless and incautious.

HOW YOU CAN BE SAFE… MAJOR PRECAUTION

“Prevention is better than cure” this very common phrase motivates us to follow the proper security plans before you get harm. So for the security of your confidential data and to avoid the miss happening with our cell phone, some security measures that are necessary to be focused by everyone are given below:

- Try: to use the latest and updated Anti-viruses.
- Try: to buy new cell phone for the use and avoid second hand.
- Try: to use password or security locks.
- Try: to use registered and add free applications.
- Try: not to share your cell phone with others.
- Try: not to turn on the Bluetooth if you are not using.

REFERENCES

[1] U. Shaw and B. Sharma, "A Survey Paper on Voice over Internet Protocol (VOIP)", International Journal of Computer Applications, Vol. 139, No. 2, pp. 16-22, 2016.

[2] J. Fang, Y. Zhu, and Y. Guan, “Voice Pattern Hiding for VoIP Communications”, In Proceedings of the 25th International Conference on Computer Communication and Networks (ICCCN 2016), Waikoloa, Hawaii, USA, August 1-4, 2016.

[3] A. Azfar, K. K. R. Choo, L. Liu, Android Mobile Voip Apps: A Survey and Examination of their Security and Privacy, Springer, Vol. 16, No. 1, pp. 73-111, 2015.

[4] M. Hussain, P. Gupta, S. Bano, V. Kulkarni, L. Perigo, and D. Williams, High-Performance and Cost-Effective VoIP Security Techniques for Operations on IPv4, IPv6, and IPv4/IPv6 Networks Capstone Research Project, 2016.

[5] J. Quittek, S. Niccolini, S. Tartarelli, and R. Schlegel, "On Spam over Internet Telephony (SPIT) Prevention," IEEE Communications Magazine, Vol. 46, pp. 80-86, 2008.

[6] N. Tiwari, "VoIP Security Issues: The Grey Shades of Internet Telephony," International Journal of Computational Science, Engineering & Technology, 2013.

[7] R. Schlegel, S. Niccolini, S. Tartarelli, and M. Brunner, "ISE03-2: SPam over Internet Telephony (SPIT) Prevention Framework," in IEEE Globecom 2006, pp. 1-6.

[8] B. Cha, S. Park, and J. Kim, Experimental Verification of Docker-Based Distributed Cloud Applications for Secured Mobile VoIP, 2016.

[9] Angelos D. Keromytis, "Voice-over-IP Security: Research and Practice", IEEE Security & Privacy, Vol. 8, No., pp. 76-78, March/April 2010.

[10] E. K. E.S. Thirunavukkarasu, "A Security Analysis in VoIP Using Hierarchical Threshold Secret Sharing," in Proceedings of the UGC Sponsored National Conference on Advanced Networking and Applications, 2015.

[11] Q. Yan, R. Yu, Q. Gong, and J. Li, Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges vol. 18, 2015.

[12] M. Y. Su and C. H. Tsai, A prevention system for spam over internet telephony, Vol. 6, 2012.

[13] D. Clarke and S. Taha Ali, “End to End Security is Not Enough”, 2017.

[14] U. Paul, A. P. Subramanian, M. M. Buddhikot, and S. R. Das, "Understanding traffic dynamics in cellular data networks," In Proceedings IEEE INFOCOM, pp. 882-890, 2011.