Security and Challenges in Voice over Internet Protocols: A Survey

Vinod Kumar¹, Om Prakash Roy²
1,2Department of EE, NERIST, Arunachal Pradesh 791109, India

¹vinodnerist@gmail.com, ²oproy61@gmail.com

Abstract. Voice over Internet Protocol (VoIP) an emerging new technologies is based on real-time communication of data by sending and receiving digital signals using Internet Protocols (IP). VoIP has become popular in business organization and scientific communities. Voice coder (Codec) named as coder and decoder, play an important role in packet switch network for transfer of audio and video data. A signalling protocol known as Session Initiation Protocol (SIP) is used for data communication between nodes in VoIP network. In this paper we survey on security related issues in VoIP communication system and covered several security attacks. We proceed with survey on all the problems that have big effects on VoIP security and challenges such as data manipulation, substitution attack, power backups, jitter, latency and delay. Finally, we conclude the paper with further research on security of VoIP communication system.

Keywords: VoIP, Security, SIP, RTP, Codec

1. Introduction
Voice over Internet Protocol (VoIP) an emerging new technologies is based on real-time communication of data by sending and receiving digital signals using Internet Protocols (IP). VoIP communication system is different than Public Switched Telephone Network (PSTN). PSTN is plain old telephone system based on circuit switching technology whereas in VoIP technology use protocols such as Session Initiation Protocol (SIP) in which text-based encoding format is used for real time data communication. Data communication with security is the demand of the present day world. Four types of communications are possible in VoIP. Firstly, computer to computer, secondly computer to phone, thirdly phone to computer and lastly, phone to phone. Simple application software like Softphone, Skype, Instant messenger need to download and installation in the computer system. Computer user need to use hardware device such as microphone. Skype is the best example for such type of service [1].

1.1. VoIP Compression Algorithms (Codecs)
Voice coders (Codecs) are named as coders and decoders. These Codecs are used in packet switch network for transfer of audio and video data. Modem is an example for codec which modulates and demodulates the audio signals, this means conversion of analog signal into digital signal and vice
versa. Codecs are defined by ITU-T for real-time voice and video communication. Table 1 below gives an example of codecs with various parameters. G.711 is best in quality and widely used codec. But one disadvantage of G.711 is that it consumes more power than other codecs [3].

Table 1. Example of Codecs with various parameters.

| Codec | Packitization Delay (ms) | Payload (bytes) | Tx Rate (pkt/s) | Bit Rate (kbps) |
|-------|---------------------------|-----------------|-----------------|-----------------|
| G.7.11 | 20                         | 160             | 50              | 64              |
| G.729  | 20                         | 20              | 50              | 8               |
| G.723  | 20                         | 20              | 34              | 5.3             |

1.2. VoIP Gateways
VoIP gateways, known as MEDIA gateways. These devices play the role of mediator between phone networks and VoIP networks. Gateway has contained minimum one phone port and one Ethernet port for each device. Gateways like Analog FXO, ISDN, Cellular Phone etc. are the best examples [4].

1.3. Protocols for VoIP Systems
Protocols are responsible for real-time data transfer over the internet, for example, use of protocols for multimedia, online television and web camera. Many signalling protocols are applicable to a VoIP solution such as SIP, TRP, RTCP, SIP-T, BICC and CMSS. Protocol selection depends on services required and equipment availability. For SIP phone access, a network with SIP protocol is mandatory [4].

![Figure 1. SIP messages registration and exchange.](image)

1.3.1. Session Initiation Protocol (SIP)
SIP is used for making phone calls using Internet. This protocol can establish multimedia sessions, user location, availability, capabilities, session setup and management. For example, in case of communication between SIP user agent and Session Border Controller (SBC). There are two number of SIP phones running on any computer system connected to internet and both can identify each other on the network. The very first message from the source is known as Register message. It is mandatory to receive message by SIP client. Figure 1 as above shows standard registration exchanged SIP message. SIP is used by the service providers such as SIP trunking for PSTN replacement, and IP Multimedia Subsystem. Additionally, SIP can also be used in enterprise communications for Instant
Messaging and Unified Communication. Furthermore, SIP can be used for as transport such as TCP, TLS, UDP and SCTP. Moreover, SIP can be defined as a Web Socket transport [5].

1.3.2. RTP and RTCP
Real Time Protocol (RTP) protocol along with signalling protocol is used to build up connections over IP network. Generally, RTP is made for voice and video transfer. There are two sessions for video transfer in real time with separate SSRC identifiers, one for audio and another for video transfer. One drawback of RTP is that it does not assures the data packets transfer accurately. Real Time Control Protocol (RTCP) is applicable along with real-time protocols for transfer of data over the large network. The Quality of Service (QoS) parameters like jitter, delay and packet loss can be observed by RTCP. RTCP is not responsible for late arrival of packets. The packet structure for RTCP is defined in the RFC 3550. Real Time Control Protocol Extended Reports (RTCP-XR) is an example for improved version of RTCP [6].

1.3.3. H.323 and VoIP gateways Protocols
H 323 is an internet protocols for transfer of audio, video and digital data over the internet. This protocol operates at one step upward from the transport layer of network. VoIP gateways can be controlled and handled by various protocols. Examples of VoIP protocol are such as Asterisk, TDMoE, LTP, Megaco, MGCP, SIP and TGCP [4, 6].

1.3.4. Transmission Control Protocol (TCP)
TCP is a reliable transport protocol which has congestion control. Also, TCP is used to transport web (HTTP) traffic, but not suitable to carry real-time communication traffic such as RTP and retransmission used to implement reliability [7].

1.3.5. Transport Layer Security(TLS)
TLS is an older version security layer between the TCP and application that provides authentication and confidentiality services. In addition, TLS can run over UDP and DTLS which can be used to generate keys for SRTP also known as DTLS-SRTP [7].

1.4. Advantages
a) Low Cost - Cost of operation of VOIP system is low to as compare to traditional PBX.
b) One terminal - A VOIP system may be integrated into one PC system for web access to more than one customers. For example, web access and multimedia session can take place at a time in single system.
c) Portability - VoIP can be used anywhere in any corner of the world and important for the users with high mobility [4].
d) Upgradation - Upgradation of VoIP technology is very easy because it is based on software.
e) Bandwidth utilization - Bandwidth is utilized effectively of compression of voice calls because it does not transport 60% silence speech.

1.5. Disadvantages
a) High Initial Cost - Because of complexity in installation, moreover, VoIP do not have single standard.
b) Complexity - Voice and data security is a big challenge because VOIP systems and data networks works together, intruders may attack a VOIP system [8].
c) Low QoS - Quality of Service is not enough due to congestion on the network.
d) Power problem: If internet connection is lost, VoIP service is not available.
1.6. **VOIP Softwares**  

a) **Vox Bridge** - For improving the quality of VoIP communication with data encryption and compression features.  
b) **VoIP client and server software** - NAT traversal software for IP communications.  
c) **Improlabs** - VOIP solution provider with cloud based bandwidth optimization service, mobile softphone and instant messaging solutions.  
d) **NetExpert** - NetExpert is a modern network resource planning system with new network technologies such as IP and VoIP. NetExpert, a Network Planner is designed to simplify the network planning, preparing network configurations [9].

1.7. **Paper Organization**  

This paper is organized in six sections, introduction part covers introduction to VoIP along with necessary codecs, gateways, protocols, advantages, disadvantages and necessary software required for VoIP system. In section 2 literature survey and section 3 covers security issues in VoIP system. Section 4 and 5 describes the challenges and problems respectively in VoIP communication. Finally, section 6 concludes the paper.

2. **Literature Survey**  

Speech quality estimation models were analysed by considering set of input features and considered distortion types for different network to produce models predicting the quality degradation. The method of detecting impairment factors for equipment was produced and models were tested on VoIP data transfer [10]. A method for shifting a model to 7-kHz network is mentioned and authors noticed the change in parameters. But further study is needed with numerical validation full band voice sample [11]. The most relevant SIP-related threats and security mechanisms is presented to overcome the SIP security issues using asterisk software for multimedia applications [12]. Authors examined some VoIP security related problems in data networks. They proposed that digital password and signature more secure in VoIP communication and protect the system from threats [13]. Speaker identification was tested on VoIP traffic and found 70–75% in accuracy. But calculated data for their findings cannot be used as full identity [14]. Portable devices like mobile phone and laptop can run multimedia applications such as VoIP. These applications require sufficient power for communication between devices on networks running the applications. The battery lifetime is important factor. The authors proposed adaptive algorithm and presented experimental studies on different codecs [2]. Problem solving of strong peer’s authentication was presented through VoIP system. Voice based applications and models were used based on SIP/SRTP VoIP protocols. Some more work is pending on this type of investigations and analysis [15]. A E-Model is proposed for voice quality evaluation as per the recommendation by the International Telecommunication Union- Telecommunication(ITU-T). Authors gives a review for various codecs used in voice transmission along with Mean Opinion Score (MOS) [3]. Authors explained 2-types of Denial of Service attacks, one flooding attack and another coordinated attacks. They suggested a model for studying SIP operation and detection of DoS attacks and described algorithms to identify DoS attacks by using the model [16]. Authors proposed several methods for VoIP security and Intrusion Prevention System(IPS) for VoIP with two modules. They found VoIP protected from spoofing attack and SIP flooding attack [17]. QoE in VoIP systems is evaluated as a MOS using an end-of-call “problem token questionnaire” (PTQ) and proven to be useful in practice [18]. An approach based on ELK and PDCA for IoT’ security risks was presented and found preserving confidentiality, integrity and availability for business. Authors produced work for utilizing a tool within the IoT followed by report but need further explore [19]. Performance evaluation method for Abstract Wireless Intrusion Detection and Prevention System (WIDPS) is proposed along with three principles of IT security as confidentiality, integrity, and availability were considered important. But perfect Bayesian Nash equilibrium for signalling games remained the future research [20]. PenQuest model for viewing information system attacks was introduced. The prototype design utilized taxonomies and security standards for cyber-attacks simulation works [21].
findings on security is analyzed for IoT devices along with tools to test these devices. They introduced a platform to identify weak points in IoT communications and found that IoT devices need analysis for security [22]. The passwords up to twelve characters long is analysed for maximum combinations. They tried to prove that password may be computed and revealed about the password not as a legitimate defence for privacy. [23]. The cybersecurity for health related data is analysed and proposed the actions in preserving the Confidentiality, Integrity, and Availability (CIA) [8].

3. Security issues in VoIP system
Security of VoIP system depends on security of its hardware and software components, means physical security like physical control of system by the people, network infrastructure and servers etc. Software components like any threats which may disturb the smooth functioning of installed software. Security issues as availability, confidentiality and integrity are defined by Central Intelligence Agency (CIA). Due to connectivity of VoIP systems with data network and sharing of software or hardware equipment, intruders gets more chances of attacks to a VOIP system as compared to other voice system such as traditional switching voice system [12]. Some of the security issues associated with VoIP system are discussed below and the types of security issues along with problems and possible solutions are shown in Table 2 below.

| Type of Security Issue                  | Problems                                                                 | Possible solutions                      |
|----------------------------------------|--------------------------------------------------------------------------|-----------------------------------------|
| Vulnerabilities for attackers          | Physical connection and gain access to network                           | User authorization implementation properly. |
| Eavesdropping                          | Privacy loss                                                             | Encrypting the data                     |
| Rogue Sets                             | Threat to confidentiality                                               | Network lock down mechanism             |
| Spoofing attack                        | Unauthorised access                                                      | Firewall configuration                  |
| Denial of Services (DoS) attacks       | False SIP invite messages and memory exhaustion                          | Packet’s source IP address on sending replies |
| Flooding-based DoS attacks             | Consumption of memory and processing resources.                          | Designing of mitigation scheme          |
| VoIP Media DoS attack                  | Non availability of transmission                                         | Firewall at hardware and software level |

3.1. Vulnerabilities for attackers
VoIP network sub systems has possibilities of vulnerabilities for attackers. Some of possibilities are same as in PSTN system. For example, in case of PSTN any physical connection can be made inside the network by the attackers to gain access to calls. Similarity in case of VoIP system attacker can gain access to physical transmission lines by using transmission control protocols (TCP/IP). VoIP system is based on computer hardware and software with operating systems like windows, Linux, Unix, Mac etc. These operating systems remain the target of hackers, ultimately VoIP systems are the part of it. Vulnerability is a big weak point in the system and a threat to a voice network. A proper user authorization implementation is necessary for protection from such type of attacks [12, 24].

3.2. Eavesdropping
Eavesdropping is related to observation and monitoring of communication between two or more devices by the attacker. In VoIP system audio and video data, fax document and credit card passwords
may be captured by the hackers for further misuse. PSTN user remains comfortable about the security of conversation. VoIP user also expect the same level of security. Encrypting the data in VoIP communication is important [13].

3.3. Rogue Sets
Rogue sets is related to gaining access to VoIP network resources, intruders can install more applications to existing VoIP networks such as malicious VoIP applications. Rogue sets attacks is a big security threats to confidentiality and integrity due to unauthorized access to VoIP network. The network administrator may initiate the lock down mechanism for allowing the installation of applications only by the authorized person [13].

3.4. Spoofing attack
In such types of attacks attacker try to access to a network by showing that the message is delivered by a trusted system by “spoofing” Internet Protocols address of concern system. This type of fraud creates confusion for nodes inside VoIP system and the attacker tries to capture credentials to claim as a legitimate system user. To prevent such spoofing problem routers must be configured by not allowing the incoming packets with the source address of local domain [5].

3.5. Denial of Services (DoS) attacks
SIP is susceptible to DoS attacks. Intruders by sending false SIP INVITE messages in bulk creates problem in VoIP system management. Computation resources like processor time and bandwidth can be exploited by attackers without acknowledgement of messages. Data flow in VoIP wireless network without any encryption results in sniffing and make data trapping easy. This is known as voice trapping and an attack against confidentiality. As a bogus registration attacker can send harmful INVITE messages to the SIP server and redirect all messages to attacker’s node. Such type of attacks causes an availability and confidentiality attack. To avoid such attack administrator may use the packet’s source IP address to discard Domain Name System (DNS) resolution overhead on messages replies [24].

3.6. Flooding-based DoS attacks
SIP use INVITE and REGISTER messages and need much processing time. The main reason behind such attack is consumption of memory and processing resources. Such type of attack can also exhaust the link bandwidth of proxy server resulting DoS attack. Designing of mitigation scheme is necessary for protection of VoIP system [16].

3.7. VoIP Media DoS attack
The attackers can flood the VoIP network equipment such as VoIP Phone with large amount of Real Time Protocol packets. This is a method to invite services from remote users to flood the network with more traffic. Such type of excess traffic on network create non availability of sufficient transmission services to the standard users, moreover, the attacker may knock about gateway connection. Electrical power supply and cooling services can be affected by attackers by disturbing VoIP network and services. Such type of attack includes equipment failure, terrorism, accident, etc. Firewall implementation at hardware and software level for detecting false stop message to media devices may be considered to avoid such attack [23, 25].

4. Challenges in VoIP Communication System
VoIP is not secure as compare to the traditional telephone systems. Before Implementation of this technology successfully, it is necessary to understand challenges associated with it [8]. Some of the challenges in VoIP communication system are shown in Table 3 along with problems associated and possible solutions.
4.1. **Data Manipulation:**
Call records are maintained in the call database known as Call Data Records (CDR). This database can be manipulated by the attackers. For example, unauthorized access to phone calls, deleting the phone numbers from database, modification of calls etc. Data manipulation is a serious matter in VoIP systems and may encourage the criminal activities. Encryption and decryption of communicating data only by authorized parties may be implemented [23].

4.2. **Address Resolution Protocol (ARP)**
By forwarding false ARP data to VoIP system, an attacker may combine his Media Access Control (MAC) number and a different Internet Protocols address in the ARP cache of attacker’s node. In this way attacker may gain access to VoIP system. To avoid such attacks, Dynamic ARP Inspection (DAI) may be useful which intercepts every ARP packet [ 24].

4.3. **Substitution attack**
In case of Substitution attack the hacker uses to capture conversations between parties and manage the alteration of some portion of speech with meaning. Such type of fraud may be happening in banking or other financial institutions to draw cash by knowing user name and passwords. Biometrics implementation may help in protecting the system from attack [26].

| Types of challenges       | Problems                                      | Possible solutions                           |
|---------------------------|-----------------------------------------------|---------------------------------------------|
| o Data Manipulation       | Deleting/modification of VoIP calls database  | Encrypting/decrypting only by authorized party |
| o Address Resolution Protocol (ARP) | Gaining access to VoIP system                 | Dynamic ARP Inspection                       |
| o Substitution Attack     | voice conversations capture and alteration   | Biometrics implementation                   |
| o Overflow in Buffer      | Move of data to another buffers               | Updating of OS time to time                 |
| o (DHCP) attack           | Alteration of IP address data by sending DHCP request | IEEE 802.1x specification provides the mechanism |
| o System Software Attack  | Installing of different OS                    | Control gateways with latest patches of OS   |
| o Backup Equipment and Power | Power failure and no backup                   | Parallel system planning                     |

4.4. **Overflow in Buffer**
In this type of attack system buffer is manipulated to hold more data than its actual size, so that data can move to the another buffers. Overflow in buffer attack may be used by the attackers for phone devices and nodes in a VoIP network. In such cases to avoid attack, operating systems like Windows, Linux must be updated time to time [27].
4.5. **Dynamic Host Configuration Protocol (DHCP) attack**
The attacker send DHCP request for MAC addresses and alter the data of IP address in the system. This may prevent the nodes for getting IP address and bound the server to obtain IP address from another VoIP server. The IEEE 802.1x specification provides a mechanism to prevent such attack [27, 28].

4.6. **System Software Attack**
System Software Attack is attack on operating system software like windows, Linux, Mac. etc. Any software for softphone may be installed on the operating system of any VoIP system. This may give chance to attacker to access important call data from the VoIP server. To avoid such attack control gateways should be implemented and latest patches of operating system must be updated [5].

4.7. **Backup Equipment and Power**
Backup power requirement is estimated based on the number of VoIP phones attached with the equipment. Emergency power requirement is estimated based on the fact that for how much long time the equipment needs to remain in working condition. VoIP network can be planned with parallel systems so that in case of failure of one equipment other equipment should start working and network traffic is not affected. Backup phones may be considered as safety measure in case of failure of IP phone for making emergency call [25].

5. **Problems in VoIP communication system**
VoIP communication can experience problem of poor call quality of voice transmission. Some of the major problems in VoIP communication system are mentioned below.

5.1. **Jitter and Latency**
Jitter is related to arrival data packets at destination not in its original sequence. In packet switched networks data packets travels in different paths from source to the destination and vice versa. Assembling and disassembling of data packets is a continues process in VoIP system during communication between two or more devices. This process degrades the voice and video quality due to data packets lost in between communication path. Jitter affect the voice and video quality of VoIP system. Latency is the time taken by a data packet to reach from its source to its destination. Latency in VoIP system is related to the time taken by voice from speaker’s mouth to listener’s year [29].

5.2. **Delay**
Three types of delays are possible in VoIP communication, the propagation Delay, handling delay and queuing delay. Time taken by light to pass through vacuum medium is 1,86,000 mps (mile/sec) and by electrons via metal like copper is about 125,000 miles per second. Fiber network induces a delay about 70 ms (milliseconds). This type of delay known as propagation delay causes in VoIP system speech quality degradation. Secondly, the handling delay, is a big issue in VoIP system as it is concerned with forwarding of frames through packet switched network. Lastly, the queuing delay where packets in data network arrived at destination in que and because of congestion, packets may not arrive at given time. Queuing delay also degrade the Voice and video quality in VoIP system [29].

5.3. **Internet Connectivity**
Generally, network is configured for data transfer, if network is not properly configured for audio and video transfer the audio and video quality may degrade. Internet Service Provider (ISP) design their networking based on web surfing, they need extra protocols for video handling. Low internet connectivity, inadequate router and internal network not configured properly are the problem need to be solved for improvement of voice quality. VoIP system needs specialised routers and their proper configuration for audio and video transfer [19].
6. Conclusion
Many organizations are adopting VoIP network as compared to traditional telephone network based on switching circuit. The reason for the choice is the VoIP implementing cost and easy to install. But security of the system is big challenge to secure confidential data from attackers. We surveyed on VoIP security and found that the security issues like as eavesdropping, rogue sets and spoofing attack etc. are big challenges against the confidentiality and integrity of data on VoIP network. We presented securities issues in VoIP system along with problems and possible solutions in the form of table. We continue with survey on possible problems and challenges that have big effect on VoIP security such as data manipulation, substitution attack, power backups, jitter, latency and delay. Moreover, we presented types of challenges along with problems and possible solutions in the form of table. It is concluded that lots of efforts are made by researcher since the inception of Voice over Internet Protocols technology to improve its voice and video quality but problems still remain. Further, researchers need to work on the security issues and challenges to provide solutions against the security attacks which are still active in present days VoIP communication systems.

References
[1] Gupta V and Dharmaraja S 2013 Reliability and performance modelling of VoIP system with multiple component failures International Journal of Reliability and Safety 7(1) 58-74
[2] Naem M, Namboodiri V and Pendse R 2010 Energy implication of various VoIP codecs in portable devices IEEE Local Computer Network Conference 196-199
[3] Chhabra A and Singh D 2015 Assessment of VoIP E-model over 802.11 wireless Mesh network IEEE International Conference on Advances in Computer Engineering and Applications 856-860
[4] Raj R, Gagneja A and Singal R 2012 Voice over Internet Protocol–The Technology and Its Application International Journal of Scientific & Engineering Research 3(5) 1-6
[5] Al Saidat, M R S, Al Kasasbeh B and Al Adwan F 2015 Develop a secure SIP registration mechanism to avoid VoIP threats IEEE International Conference on Open Source Software Computing 1-6
[6] Jalandry S and Verma S 2015 A detail review on voice over internet protocol (voip) Int. J. Eng. Trends Technol 23(4) 161-166
[7] Lam T, Galkandage C, Dagiuless T and Iqbal M 2020 Much needed Group-based Quality of Experience on Unified Communications to support post COVID-19 Disruptive Business Models State-of-the-Art and Research Challenges 1-17
[8] Okereafor K and Marcelo A 2020 Addressing Cybersecurity Challenges of Health Data in The Covid-19 Pandemic International journal in IT & Engineering 8(6) 1-12
[9] Castanon G, Sarmiento, A M, Ramirez-Velarde R and Aragón-Zavala A 2009 Software tool for network reliability and availability analysis Wire Journal International 74 1-12
[10] Raja A, Azad R M A, Flanagan C and Ryan C 2008 VoIP speech quality estimation in a mixed context with genetic programming Proceedings of the 10th annual conference on Genetic and evolutionary computation (ACM) 1627-1634
[11] Myakotnykh E S and Thompson R A 2009 Computational quality model for wideband voice-over-IP communications IEEE International Workshop Technical Committee on Communications Quality and Reliability 1-6
[12] Werapun W, Abou El Kalam A, Paillassa B and Fasson J 2009 Solution analysis for SIP security threats IEEE International Conference on Multimedia Computing and Systems 174-180
[13] Maher A, Hegazy A F, Hasan B and Hashim M 2010 Beyond steganography for Voice Over IP (VOIP) IEEE International Conference on Computer Engineering & ystems 46-51
[14] Khan L A, Baig M S and Youssef A M 2010 Speaker recognition from encrypted VoIP communications Digital Investigation 7(1-2) 65-73
[15] Cattaneo G, Catuogno L, Petagna F and Roscigno G 2015 Reliable voice-based transactions over VoIP communications *IEEE 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing* 101-108

[16] Golait D and Hubballi N 2016 Detecting anomalous behavior in VoIP systems: A discrete-event system modeling *IEEE Transactions on Information Forensics and Security* **12**(3) 730-745

[17] Chen M J, Wen C C, Lin H C and Chu Y S 2016 ASIC design and implementation for VoIP intrusion prevention system *IEEE International Conference on Applied System Innovation* 1-4

[18] Gupchup J, HosseinKashi Y, Ellis M Johnson S and Cutler R 2017 Analysis of problem tokens to rank factors impacting quality in VoIP applications *IEEE Ninth International Conference on Quality of Multimedia Experience* 1-6

[19] Abbass W, Bakraouy Z, Baina A and Bella M 2019 Assessing the Internet of Things Security Risks *Journal of Communications* **14**(10) 958-964

[20] Mahini H and Mousavarad S M 2020 WiFi Intrusion Detection and Prevention Systems Analyzing A Game Theoretical Perspective *International Journal of Wireless Information Networks* **27**(1) 77-88

[21] Luh R, Temper M, Tjoa S, Schrittweiser S and Janicke H 2020 PenQuest: a gamified attacker/defender meta model for cyber security assessment and education *Journal of Computer Virology and Hacking Techniques* **16**(1) 19-61

[22] Waraga O A, Bettayeb M, Nasir Q and Talib M A 2020 Design and implementation of automated IoT security testbed *Computers and Security* **88** 101648

[23] Almuairfi S J and Alenezi M 2020 Anonymous Authentication for Privacy Preserving of Multimedia Data in the Cloud *Handbook of Research on Multimedia Cyber Security* (IGI Global) 48-72

[24] Rippon W J 2006 Threat assessment of IP based voice systems *1st IEEE Workshop on VoIP Management and Security* 19-28

[25] Chong H M and Matthews H S 2004 Comparative analysis of traditional telephone and Voice-over-Internet Protocol (VoIP) systems *IEEE International Symposium on Electronics and the Environment* 106-111

[26] Liu Z H and Wang H X 2014 Pseudo-zernike moments-based audio content authentication algorithm robust against feature-analysed substitution attack *Multimedia tools and applications* **70**(3) 2271-2291

[27] Butcher D, Li X and Guo J 2007 Security challenge and defense in VoIP infrastructures *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* **37**(6) 1152-1162

[28] Hubballi N and Tripathi N 2017 A closer look into DHCP starvation attack in wireless networks *Computers and Security* **65** 387-404

[29] Meddahi A and Afifi H 2006 Packet-E-Model: E-Model for VoIP quality evaluation *Computer Networks* **50**(15) 2659-2675