Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 8, pp. 2989–2999
DOI : 10.47974/JDMSC-2443

Cybersecurity in voice over IP (VoIP) systems : Protecting communication networks from threats, vulnerabilities, and cyber attacks

Ashish Tiwari [#]
Babu Banarsi Das Institute of Technology and Management
Lucknow Campus
Lucknow 226028
Uttar Pradesh
India

Sushanth Chandra Addimulam [†]
Kforce Inc
2681 Sidney St
Pittsburgh
PA 15203
U.S.A.

Nilesh Dubey [§]
Department of Computer Science and Engineering
Devang Patel Institute of Advance Technology and Research
FTE, CHARUSAT University
Anand 388421
Gujarat
India

K. Kiran Kumar [‡]
Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Vaddeswaram 522501
Andhra Pradesh
India

[#] *E-mail:* er.ashish.tiwari89@gmail.com
[†] *E-mail:* sushanth93@gmail.com
[§] *E-mail:* nileshdubey.ce@charusat.ac.in
[‡] *E-mail:* kiran5434@kluniversity.in

Dhiraj Kapila [@]
Department of Computer Science & Engineering
Lovely Professional University
Phagwara 144411
Punjab
India

Kusumlata Jain *
Department of Computer & Communication Engineering
School of Computer Science and Engineering
Manipal University
Jaipur 303007
Rajasthan
India

Abstract

Voice over Internet Protocol (VoIP) technology facilitates voice communication over IP networks, offering a more affordable and adaptable alternative to traditional phone systems. However, VoIP comes with substantial cybersecurity risks, including threats like eavesdropping, denial of service (DoS) attacks, man-in-the-middle attacks, spoofing, and fraud. As VoIP becomes increasingly prevalent in both personal and business contexts, securing these systems is paramount. This paper examines the vulnerabilities associated with VoIP, outlines common attack vectors, and discusses security strategies such as encryption, authentication protocols, firewalls, and intrusion detection systems aimed at mitigating these risks. The study concludes by offering recommendations for enhancing VoIP security through a combination of advanced technology and best practices.

Subject Classification: *Primary: 68M25, Secondary: 94A60, 68P25.*

Keywords: *VoIP security, Cybersecurity, Communication networks, Threat mitigation, VoIP vulnerabilities, Network security, Encryption, SIP security, Denial-of-service (DoS) attacks, Fraud prevention, Secure VoIP protocols, Authentication, Intrusion detection, Telecommunication security.*

1. Introduction

Voice over Internet Protocol (VoIP) is a technology that facilitates voice communication by transforming voice signals into digital data packets for transmission over the internet. In recent years, it has become increasingly popular due to its affordability, flexibility, and user-friendliness when compared to traditional telephone systems [1-2].

[@] *E-mail:* **dhiraj.23509@lpu.co.in**
* *E-mail:* **kusumlata.jain@jaipur.manipal.edu (Corresponding Author)**

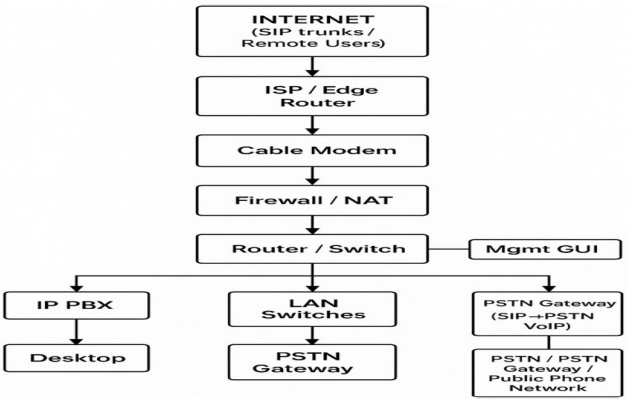

Figure 1

VoIP System.

However, since VoIP operates via the internet, it is exposed to various cybersecurity risks, such as eavesdropping, data breaches, call manipulation, service interruptions, and other cyberattacks [3]. The transition from conventional Public Switched Telephone Networks (PSTN) to VoIP introduces additional security challenges, as VoIP heavily depends on internet infrastructure, which is more susceptible to security threats as shown in figure 1. These vulnerabilities stem from the complexity of VoIP protocols like Session Initiation Protocol (SIP) and Real- Time Protocol (RTP), its integration with other internet- based services, and reliance on IP networks [4-5]. VoIP services convert voice into a digital signal that travels over the Internet. If you call a standard phone number, the signal is transformed into an analog telephone signal before reaching the recipient [6-7]. With VoIP, you can make calls directly from a computer, use a special VoIP phone, or connect a traditional phone via a special adapter. Wireless hotspots in places like airports, hospitals, and cafes provide Internet access, allowing you to use VoIP services wirelessly [8-9].

2. Literature Review

Traditional telephones operate by transmitting voice signals over centralized public telephone exchanges through electronic signals, with a dedicated call connection maintained throughout the conversation [1]. In contrast, VoIP relies on a packet-switched network, such as the Internet or a private LAN, rather than the circuit- switched networks used by PSTN. While the Internet often utilizes the telephone network, other connection

options like cable or wireless Internet are also available [10-11]. Both software-based and some hardware VoIP solutions use standard Internet connections (IP connections), but VoIP calls may not always have a guaranteed connection [6]. Technically, VoIP breaks conversations into "IP packets," which are transmitted separately over various network paths, including the Internet [12-13]. A broadband Internet connection and a computer workstation or laptop are necessary. Users can often make and receive free calls to others within the same softphone network [14-15]. Some services allow the use of a 'username' instead of a traditional phone number, although regular phone numbers may also be provided. The functionality and reliability of softphones may not match that of other solutions [16-17]. Softphones are increasingly appearing in the mobile device market, including PDAs and 3G mobile phones. Specifically designed for business-grade applications, this system necessitates various infrastructure upgrades and placements [18-19]. It typically comes at a higher cost compared to software-based VoIP solutions. Offering high functionality, reliability, and quality of service, it also provides robust security and scalability [20-21]. This solution is ideal for environments that require more than 10 separate endpoint handsets. Additionally, it often necessitates the involvement of an IT specialist, either in-house or through a service provider, to assess business needs and customize an appropriate solution [22-23]. VoIP handsets / adapters, Instand Messaging voice services and Mobile VoIP are major solutions given [24].

3. Voip Threats- Integrity

A "man-in-the-middle" attack refers to the interception, modification, and retransmission of messages within a trusted conversation. In certain VoIP systems, data is sent as packets over shared computer networks, including the Internet, where it shares pathways with various types of traffic and is more easily accessible. If not adequately secured, attackers can manipulate or distort the content of messages, rendering them unusable or unrecognizable. This manipulation can extend to altering voicemail, fax, and other messaging services through VoIP, as well as reconstructing video content [3]. Individuals without authorization might impersonate another user by redirecting their telephone calls. If an unauthorized individual manages to access the necessary Internet connections, they can reroute VoIP calls from any location globally to any other location worldwide. To operate, softphones need a workstation. The primary attack vectors for this platform include vulnerabilities found in

the softphone application, the operating system, the network, and potential attacks targeting your service provider. Protecting softphones can be challenging, as users typically have limited control over the application's configuration shown in figure 2. Therefore, it's essential for users to carefully evaluate their choice of softphone, especially regarding the protocols it supports. For workstation softphones, it's advisable to choose those that utilize SIP and SRTP protocols; most vendors indicate whether their softphones support these or can provide that information upon request. When implemented effectively by the vendor, both protocols can significantly enhance the security of VoIP services [7]. Recent advancements in softphone security focus on third-party end-to-end VoIP security solutions. These solutions create secure channels for the entire duration of a call, ensuring protection from the caller to the receiver and back. It is advisable to install these applications, as they significantly enhance confidentiality and integrity compared to softphones lacking such protection [5]. Typically, both endpoints must have security solution installed for effective end-to-end protection.

Using a softphone over public and unsecured networks, such as free Wi-Fi or Internet cafes, can lead to security vulnerabilities. If you are on a workstation that hasn't been properly secured or is not owned by the VoIP-enabled SME, the confidentiality of your calls may be at risk. To enhance security while using VoIP on public networks, it is advisable to use a VPN or another end-to-end VoIP solution. User options for securing VoIP adapters, routers, and modems are often limited to the features provided by VoIP vendors [3]. However, choosing products with strong security protocols, such as SIP and SRTP, can greatly enhance VoIP system security. For mobile and wireless VoIP devices, security measures resemble those for softphones but require additional precautions due to the wireless nature of the connections. Proposed Algorithm: Secure VoIP

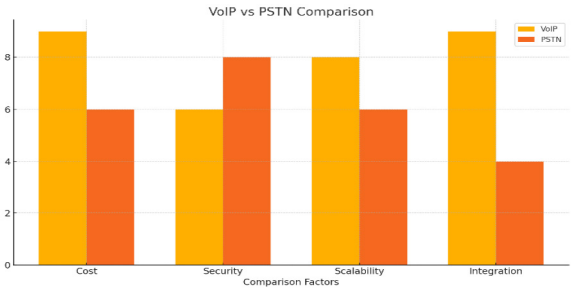

Figure 2

VoIP vs PSTN comparison.

Communication System. Input: VoIP network traffic (SIP/RTP packets). User authentication requests. Call setup and termination signals. Network activity logs. Output: Secure and encrypted VoIP communication. Mitigation of cyber threats and vulnerabilities. Real-time threat detection and response.

Step 1: User Authentication & Access Control. Verify user identity using Multi-Factor Authentication (MFA). Implement Role-Based Access Control (RBAC) for VoIP network resources. Use strong SIP authentication (Digest Authentication, TLS certificates). Step 2: Encryption & Secure Communication. Encrypt SIP signaling using TLS (Transport Layer Security). Encrypt RTP voice traffic using SRTP (Secure Real-time Transport Protocol). Deploy End-to-End Encryption (E2EE) for private VoIP calls. Step 3: Network Security & Firewall Protection. Configure Session Border Controllers (SBCs) to filter malicious SIP traffic. Implement VoIP-aware firewalls with Deep Packet Inspection (DPI). Block unauthorized SIP requests from untrusted IP addresses. Step 4: Threat Detection & Intrusion Prevention. Monitor network logs for abnormal call patterns (e.g., high call rates, unusual destinations). Use Intrusion Detection Systems (IDS) to detect DoS (Denial-of-Service) attacks. Implement AI/ML-based anomaly detection to identify fraudulent activities. Step 5: VoIP Fraud Prevention & Security Policies. Enable call rate limits and geo-restrictions to prevent toll fraud. Use honeypots to detect and study VoIP attack patterns. Enforce regular security audits and compliance with VoIP security standards. Step 6: Real-Time Response & Incident Handling. Upon detecting an attack, block malicious IPs and suspend compromised accounts. Notify administrators with detailed logs of suspicious activities. Perform forensic analysis post-attack to strengthen security policies. Step 7: Continuous Security Monitoring & Updates. Apply regular software updates and patches for VoIP servers and endpoints. Conduct penetration testing and vulnerability assessments on VoIP infrastructure.

The primary goals of VoIP include reliability, interoperability, and quality of service. As a result, security considerations were often secondary in the initial implementations of VoIP. However, this has led to several significant security challenges that VoIP systems face. Transmission over IP/Internet VoIP shares the same infrastructure as data services, which exposes it to common data security vulnerabilities, as well as issues that are specific to VoIP. VoIP lacks a standardized protocol for the transmission and reception of information. Although there have been only a limited number of publicly reported security incidents specifically involving VoIP

systems, it is crucial for organizations to prioritize the security of their VoIP solutions. Doing so helps mitigate the risks and threats associated with VoIP, as outlined in the Threats section of this booklet. Security must be a key consideration for any small to medium- sized enterprise (SME) that has either already implemented a VoIP solution or is in the process of doing so, as it represents an important aspect of investing in new technology.

In VoIP architecture, voice communications are transmitted over the Internet in the form of data packets. If these packets are not encrypted, attackers could potentially intercept and interpret the information they contain. Traffic analysis can reveal information about network structures and call patterns. Since VoIP devices must be available to receive connections, such as telephone calls, attackers might detect these devices on your network. They can then use specialized software, like SIPtap, to monitor VoIP calls. This enables them to acquire critical details regarding your organization's physical layout, operational processes, and contact information for clients and suppliers. Many VoIP systems now offer a voicemail feature similar to that found in traditional telephony services. However, this voicemail function can be vulnerable to confidentiality attacks, allowing unauthorized access to its contents. By implementing encryption and access controls, VoIP voicemail can achieve a higher level of security compared to standard telephony voicemail systems.

4. Computer Security Essentials

For security purposes, using a supported operating system and keeping it up to date with the latest patches is crucial. By utilizing personal firewall software, users can safeguard their computers against hackers and block unauthorized programs from gaining access. While some individuals may think their data isn't valuable enough to attract hackers, there are numerous other motives for cybercriminals to attempt to infiltrate systems. Therefore, it's essential for all computers connected to the Internet to employ a firewall. Even infrequent users face the same risks as those who are online full-time, as both can be targets of random hacker scans. Anti-virus software prevents harmful viruses from infiltrating computers and devices like PDAs and mobile phones. Viruses, which are essentially software programs, vary in their effects based on their programming and intent. Some are intentionally created to corrupt files or disrupt computer operations, posing a risk of damaging or erasing data on a hard disk. In addition to real-time protection, regular full virus scans are essential for

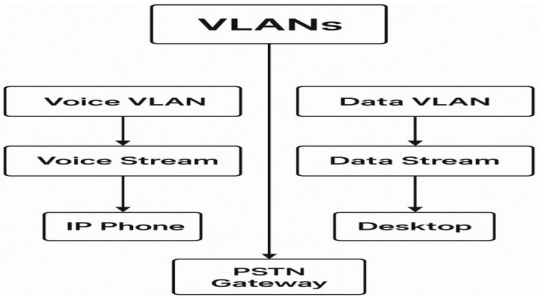

Figure 3

Separating voice streams and data streams in VLANs.

maintaining system integrity; these scans can be scheduled to run at convenient times. Spyware is a type of software designed to collect personal information for marketing, advertise, or modify a computer's settings without the user's permission described in figure 3. Unexpected pop-up ads, even when offline. Unfamiliar changes to the homepage of the web browser. New toolbars or components in the browser that the user does not recall installing. A noticeable decrease in overall system performance or delays in task completion. Altered settings that the user cannot revert. Establishing a backup strategy is crucial for safeguarding data, as data loss can occur for various reasons beyond security breaches, such as power outages, hardware malfunctions, and human errors. Regularly backing up files offers the best defense against these threats. Organizations must choose a backup schedule, decide on storage options, and select a backup method, which could include utilizing a remote service or manually saving to a portable hard drive. Regardless of whether backups are handled in-house or outsourced, a backup schedule must be established, considering these techniques like this involves creating a complete copy of all data and system files. It is not necessary to perform this daily, as most files do not change frequently. This type captures all files that have been altered since the last full backup.

This method is efficient in terms of time and storage space; however, restoring data in case of loss requires accessing multiple backups in the correct sequence.

5. Conclusion

This research has explored the application of blockchain technology in enhancing transparency within supply chains. Blockchain's

decentralized and immutable nature offers a robust solution to address critical challenges such as data manipulation, lack of traceability, and inefficiencies that currently plague global supply chains. The research findings suggest that integrating blockchain into supply chain management can significantly improve transparency, accountability, and trust among stakeholders by ensuring real-time, tamper-proof records of transactions. However, challenges remain in terms of scalability, regulatory compliance, and the need for widespread industry adoption. The successful implementation of blockchain solutions will depend on addressing these barriers through collaborative efforts between technology developers, policymakers, and industry leaders. Future research can focus on enhancing the efficiency of blockchain protocols and exploring hybrid systems that combine blockchain with other emerging technologies, such as IoT and AI, to further optimize supply chain operations.

References

[1] R. Dantu and P. Kolan, "Detecting spam in VoIP networks," in *Proceedings of the Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI)*, pp. 31–37 (2005).

[2] D. Zhu and J. Zhang, "VoIP security: Problems and solutions," in *2014 International Conference on Information Technology and Management Innovation (ICITMI)*, pp. 15–19 (2014).

[3] E. Y. Chen and D. Zhou, "Mitigating VoIP vulnerability to Denial of Service (DoS) attacks," *Security and Communication Networks*, vol. 5, no. 12, pp. 1421–1432 (2012).

[4] S. Fahad and A. Hamza, "Machine learning approaches for spam detection in online social networks," *Artificial Intelligence Review*, vol. 54, no. 5, pp. 3141–3174 (2021).

[5] Y. V. Rangaiah, A. K. Sharma, T. Bhargavi, M. Chopra, C. Mahapatra, and A. Tiwari, "A taxonomy towards blockchain-based multimedia content security," in *2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT)*, pp. 1–4, IEEE (Dec. 2022).

[6] N. K. Singh, A. Jain, S. Arya, W. E. G. Gonzales, J. E. A. Flores, and A. Tiwari, "Attack detection taxonomy system in cloud services," in *2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT)*, pp. 1–5, IEEE (Dec. 2022).

[7] A. Tiwari and R. Garg, "Reservation System for Cloud Computing Resources (RSCC): Immediate reservation of the computing mechanism," *International Journal of Cloud Applications and Computing (IJCAC)*, vol. 12, no. 1, pp. 1–22 (2022).

[8] A. Tiwari and R. M. Sharma, "Potent cloud services utilization with efficient revised rough set optimization service parameters," in *Proceedings of the International Conference on Advances in Information Communication Technology & Computing*, pp. 1–7 (Aug. 2016).

[9] A. Tiwari and R. M. Sharma, "Realm towards service optimization in fog computing," in *Research Anthology on Architectures, Frameworks, and Integration Strategies for Distributed and Cloud Computing*, IGI Global, pp. 1530–1563 (2021).

[10] H. Mehraj and M. S. Malik, "Text mining for spam detection: An overview," *Journal of Theoretical and Applied Information Technology*, vol. 97, no. 11, pp. 3036–3044 (2019).

[11] N. Ishak and M. Haris, "Effective spam filtering using machine learning algorithms: A comparative study," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 8, pp. 534–541 (2020).

[12] R. Kumar and A. Sahu, "A review of spam detection techniques: Challenges and future directions," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 6, pp. 635–645 (2020).

[13] A. D. Clark, "VoIP security: Attacks and solutions," *International Journal of Computer Applications*, vol. 45, no. 21, pp. 15–19 (May 2017).

[14] K. Chakraborty, S. Singhal, N. Arya, M. Tiwari, A. Khatoon, and A. Tiwari, "Multilevel cloud resource scheduling approach based on image-based signature system," in *Proceedings of the 5th International Conference on Information Management & Machine Intelligence (ICIMMI)*, pp. 1–7 (Nov. 2023).

[15] A. Tiwari and R. Garg, "Adaptive ontology-based IoT resource provisioning in computing systems," *International Journal on Semantic Web and Information Systems (IJSWIS)*, vol. 18, no. 1, pp. 1–18 (2022).

[16] D. Dudeja, S. M. Sabharwal, Y. Ganganwar, M. Singhal, N. Goyal, and A. Tiwari, "Sales-based models for resource management and scheduling in artificial intelligence systems," *Engineering Proceedings*, vol. 59, no. 1, pp. 43 (2023).

[17] A. Tiwari and R. M. Sharma, "A skywatch on the challenging gradual progression of scheduling in cloud computing," in *Applications of Computing, Automation and Wireless Systems in Electrical Engineering: Proceedings of MARC 2018*, Springer Singapore, pp. 531–541 (2019).

[18] R. Manikandan, R. K. Maurya, T. Rasheed, S. C. Bose, J. L. Arias-Gonzáles, U. Mamodiya, and A. Tiwari, "Adaptive cloud orchestration resource selection using rough set theory," *Journal of Interdisciplinary Mathematics*, vol. 26, pp. 311–320 (2023).

[19] A. Tiwari and R. Garg, "ACCOS: A hybrid anomaly-aware cloud computing formulation-based ontology services in clouds," in *Proceedings of ISIC Conference*, pp. 341–346 (2021).

[20] S. Kumar, S. Kumar, N. Ranjan, S. Tiwari, T. R. Kumar, D. Goyal, M. K. Rafsanjani, and others, "Digital watermarking-based cryptosystem for cloud resource provisioning," *International Journal of Cloud Applications and Computing (IJCAC)*, vol. 12, no. 1, pp. 1–20 (2022).

[21] S. Kumar, P. K. Srivastava, G. K. Srivastava, P. Singhal, D. Singh, and D. Goyal, "Chaos-based image encryption security in cloud computing," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 4, pp. 1041–1051 (2022).

[22] S. Kumar, K. K. Dubey, A. K. Gautam, S. Verma, V. Kumar, and U. Mamodiya, "Detection of recurring vulnerabilities in computing services," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 4, pp. 1063–1071 (2022).

[23] S. Kumar, P. K. Srivastava, A. K. Pal, V. P. Mishra, P. Singhal, G. K. Srivastava, and U. Mamodiya, "Protecting location privacy in cloud services," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 4, pp. 1053–1062 (2022).

[24] M. Malik, M. Kumar, V. Kumar, A. K. Gautam, S. Verma, S. Kumar, and D. Goyal, "High-level browser security in cloud computing services from cross-site scripting attacks," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 4, pp. 1073–1081 (2022).

Received February, 2025