INTERNATIONAL JOURNAL OF SMART SYSTEMS
Volume 1 Issue 3 Year 2023 Pages 105 - 116
e–ISSN 2986-5263
Url: https://ijss.etunas.com/index.php/ijss/index

# Security Analysis of the VoIP (Voice Over Internet Protocol) System

**Alya Wulan Apriliyani[1]*, Rakhmadi Rahman [2], Desvi[3]**
Bacharuddin Jusuf Habibie Institute of Technology, Parepare, Indonesia

*Correspondence to: alyawulanapriliyani0404@gmail.com

**Abstract:** Voice over Internet Protocol (VoIP) is a communication technology that enables voice transmission over IP-based networks, offering advantages such as cost efficiency, flexibility, and service integration. Despite its benefits, VoIP faces significant security vulnerabilities due to its open architecture and dependence on public internet infrastructure. This study presents a literature-based analysis of the primary security threats targeting VoIP systems, including eavesdropping, Denial of Service (DoS) attacks, spoofing, session hijacking, and Network Address Translation (NAT) traversal problems. The research also discusses a range of countermeasures, including Secure Real-time Transport Protocol (SRTP), Transport Layer Security (TLS), Intrusion Detection and Prevention Systems (IDS/IPS), adaptive firewalls, and robust authentication protocols such as STIR/SHAKEN. While these technical solutions are effective, their success depends on proper implementation and continuous system monitoring. Although there may be minor trade-offs in performance, particularly in latency, such compromises are acceptable under global standards to ensure secure communication. The findings underscore the importance of a layered security strategy that maintains both protection and Quality of Service (QoS), making VoIP a dependable solution for critical sectors such as government, finance, and business.

**Keywords:** VoIP security; SRTP; DoS attack; intrusion detection; session hijacking; network security.

**Article info:** Date Submitted: 12/07/2023 | Date Revised: 13/08/2023 | Date Accepted: 24/08/2023



## INTRODUCTION

The rapid advancement of information and communication technology has significantly transformed the way humans communicate, particularly in the domain of voice communication[1]. One of the most groundbreaking innovations in this field is Voice over Internet Protocol (VoIP), a technology that allows voice transmission over IP-based networks such as the internet. Unlike traditional communication systems like the Public Switched Telephone Network (PSTN), which depend on dedicated and costly telecommunication infrastructures[2], VoIP utilizes existing internet infrastructure, offering greater flexibility, reduced costs, and seamless integration with other digital services. VoIP is now widely adopted across various sectors ranging from individual users and small businesses to large-scale enterprises and government institutions due to its affordability, scalability, and multi-platform compatibility[3].



https://doi.org/10.63876/ijss.v1i3.69

Despite these numerous advantages, VoIP also presents unique challenges, particularly in terms of security. Because VoIP operates over open and public networks, it is inherently more vulnerable to cyber threats compared to traditional telephony systems, which are typically isolated from the internet. This shift from closed to open communication channels exposes VoIP systems to a variety of malicious activities, including eavesdropping, spoofing, call hijacking, Denial of Service (DoS) attacks, and unauthorized access to sensitive voice data. These threats not only jeopardize the confidentiality, integrity, and availability of communications but also put users both individuals and organizations at risk of serious data breaches, identity theft, and operational disruptions[4].

The urgency of addressing VoIP security issues becomes even more pronounced in critical sectors such as finance, healthcare, and government, where the protection of information and communication systems is paramount. Several studies have previously explored the technical and operational aspects of VoIP, with a focus on protocol efficiency, call quality, and cost-effectiveness. However, there remains a considerable research gap in comprehensive analyses that emphasize the security vulnerabilities of VoIP and the strategic implementations required to mitigate such threats. Most existing literature tends to treat security as a secondary concern, leaving behind a pressing need for a focused investigation on the defense mechanisms necessary to secure VoIP infrastructures in both enterprise and public domains[5].

Notably, protocols like the Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP)[6][5] which serve as the foundational frameworks for VoIP communication are known to possess inherent security limitations. Studies indicate that while these protocols are efficient for establishing and managing multimedia sessions, they lack robust built-in security features, making them attractive targets for attackers. Several real-world incidents have demonstrated how vulnerabilities in SIP signaling or RTP data streams can be exploited to compromise entire VoIP ecosystems. Thus, understanding the weaknesses embedded in these protocols is crucial for enhancing overall system security[7].

In response to these gaps, recent developments have focused on the implementation of security protocols such as Secure RTP (SRTP), Transport Layer Security (TLS), and IPsec to protect voice communication traffic. Additionally, specialized security tools like VoIP-aware firewalls, Intrusion Detection Systems (IDS), and behavior-based anomaly detection algorithms are being proposed as effective countermeasures. Despite these advancements, the adoption of such technologies remains inconsistent, particularly in small and medium-sized enterprises (SMEs) that often lack the technical expertise or financial resources to deploy comprehensive security frameworks[8][5].

This research is motivated by the urgent need to bridge the gap between theoretical knowledge and practical implementation in the realm of VoIP (Voice over Internet Protocol) security. As digital communication technologies continue to evolve rapidly, VoIP has emerged as one of the most widely adopted solutions for voice communication across both individual and organizational levels. While this technology offers significant advantages including cost efficiency, flexibility, and seamless integration with other digital services it also introduces a wide range of security vulnerabilities that are often overlooked. Many existing studies and implementations focus primarily on the functional and operational efficiency of VoIP, while security aspects remain underexplored, especially in practical, real-world environments. Therefore, this research aims to provide a comprehensive and systematic analysis of the key security threats that VoIP systems face today. These threats include eavesdropping (interception of voice data), spoofing (forging user identities), Denial of Service (DoS) attacks that disrupt communication, and manipulation of voice data that compromises the integrity of information. Beyond identifying these risks, the study also seeks to examine and evaluate current preventive measures such as the use of Secure Real-time Transport Protocol (SRTP), Transport Layer Security (TLS), VoIP-specific firewalls, and Intrusion Detection Systems (IDS)[9].



https://doi.org/10.63876/ijss.v1i3.69

However, while these technologies and strategies are available, not all of them prove to be effective across different operational contexts. One of the core objectives of this research is to assess how well these existing solutions perform when implemented in various real-world scenarios, including enterprise networks, government agencies, and individual user environments[10]. The evaluation process considers constraints such as limited resources, varying levels of technical expertise, and infrastructure complexities. As a result, the findings are expected to provide a realistic and applicable perspective on how VoIP security measures can be optimized for different use cases[11]. To maintain a balanced approach, this study combines both theoretical and practical perspectives. On the theoretical side, it explores protocol vulnerabilities in systems such as Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP), as well as encryption and authentication standards that are critical to securing VoIP communication. On the practical side, it investigates applied strategies such as system hardening, continuous network monitoring, and the implementation of proactive threat detection mechanisms. This dual approach ensures that the research does not merely describe the issues but also offers actionable recommendations for mitigating risks. Overall, this study not only contributes to academic knowledge in the field of VoIP security but also serves as a practical guide for IT professionals, network administrators, and policymakers who are responsible for managing communication infrastructures[12][13]. By integrating theory with application, the research aspires to support the development of VoIP systems that are not only efficient and scalable but also robust and secure. The expected outcome is a set of evidence-based, practical recommendations that organizations can adopt to enhance their VoIP implementations boosting operational reliability and user trust in internet-based voice communication systems.Furthermore, the increasing reliance on VoIP as a central mode of communication especially in the post-pandemic digital transformation era demands heightened awareness and preparedness among IT professionals and system administrators. As cyberattacks grow more sophisticated, the implementation of proactive and layered security strategies becomes not only beneficial but essential. Therefore, understanding how to design, deploy, and manage secure VoIP systems is a valuable competency in the modern digital landscape[14][15].

To this end, this study seeks to answer several core research questions:

1. What are the most significant security threats in VoIP systems?
2. How do VoIP protocols like SIP and RTP contribute to system vulnerabilities?
3. What countermeasures and security techniques can be applied to mitigate these threats effectively?

By addressing these questions, the study aims to contribute to the growing body of knowledge on VoIP security while offering actionable insights for the development of more resilient and secure communication systems. The expected outcome is a set of practical recommendations that can guide organizations in strengthening their VoIP implementations, thereby enhancing both operational efficiency and user trust in internet-based voice communication technologies.

## RELATED WORK

### A. Definition of VoIP

Voice over Internet Protocol (VoIP) is a communication technology that enables the transmission of voice over IP networks[16], such as the internet or local area networks (LAN). Unlike traditional telephones that use circuit switching, VoIP converts voice signals into digital data packets transmitted over computer networks[17]. This technology offers a more cost-effective, flexible, and integrated voice and data communication service[18]. End-user devices include IP phones, softphones, and gateways[19]. VoIP servers manage registration and call control functions. The main advantage of VoIP lies in its ability to unify voice and data within a single infrastructure, thereby reducing operational costs and enhancing communication capabilities[20].



https://doi.org/10.63876/ijss.v1i3.69

### B. VoIP Architecture and Components

The VoIP system architecture consists of several integrated components designed to facilitate efficient voice communication over IP networks, replacing conventional PSTN systems. The primary components include [8]:

1. Endpoint
   Devices such as IP phones and softphones that serve as communication endpoints. An IP phone is a hardware device connected to the LAN via Ethernet or Wi-Fi and equipped with codecs to digitize voice signals. A softphone is software running on a computer or smartphone that uses internal audio devices.
2. SIP Server
   The core signaling server that manages user registration, call routing, session management, and authentication. Popular SIP servers include Asterisk, FreePBX, Kamailio, OpenSIPS, and 3CX.[9]
3. Media Gateway
   A bridge between VoIP networks and traditional telephone networks (PSTN/ISDN), converting signal formats and protocols to ensure interoperability[21].
4. Communication Protocols
   These include SIP for signaling, RTP for real-time media transport, RTCP for quality control, as well as legacy protocols like H.323, MGCP, and SCCP, which ensure interoperability and session management.

### C. Key Protocols in VoIP

Voice over Internet Protocol (VoIP) technology relies heavily on two main protocols: Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP)[22].

1. SIP (Session Initiation Protocol)
   SIP is a signaling protocol used to initiate, modify, and terminate multimedia communication sessions, including voice, video, and instant messaging. Developed by the Internet Engineering Task Force (IETF), SIP enables user discovery, call setup, and dynamic session parameter management. SIP operates using request and response methods similar to HTTP and SMTP and can function over transport protocols like UDP, TCP, or SCTP. SIP defines various message types such as INVITE (to start a session), ACK (to confirm receipt of a response), BYE (to terminate a session), and REGISTER (to register user location). These messages facilitate communication between users and servers in a VoIP network. SIP also supports extensions for additional services like instant messaging and presence sharing.
2. RTP (Real-time Transport Protocol)
   RTP is designed to transmit real-time data such as voice and video over IP networks. It provides mechanisms for packet sequencing and timestamping, essential for maintaining media quality and synchronization between media streams. RTP is commonly paired with the RTP Control Protocol (RTCP), which provides feedback on transmission quality and assists in media stream synchronization. RTP typically runs over UDP, allowing efficient data delivery with minimal overhead. However, RTP itself does not guarantee Quality of Service (QoS); therefore, it is often used alongside protocols that support QoS, such as RSVP or MPLS.

### D. Security Mechanisms in VoIP

VoIP systems face numerous security risks that can compromise the confidentiality, integrity, and availability of voice communications. To safeguard VoIP systems against these threats, several preventive measures are implemented, including encryption, firewalls and intrusion



https://doi.org/10.63876/ijss.v1i3.69

detection/prevention systems (IDS/IPS), Virtual Private Networks (VPN), Network Address Translation (NAT), authentication, and access control[23].

1. Encryption: SRTP and TLS
   Encryption is vital for protecting voice data and signaling in VoIP communications. Secure Real-time Transport Protocol (SRTP) encrypts voice media streams, while Transport Layer Security (TLS) encrypts signaling messages to prevent eavesdropping or tampering. SRTP protects against replay attacks and ensures data integrity, while TLS secures signaling by providing authentication and encrypted communication channels.
2. Firewall and IDS/IPS
   Firewalls regulate network traffic based on ports and protocols to restrict unauthorized access to VoIP systems. Additionally, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) monitor and analyze network activity to detect and block potential threats such as SIP flooding attacks or suspicious port scans.
3. VPN and NAT
   Virtual Private Networks (VPN) encrypt data tunnels, protecting VoIP communication from interception over public networks. Network Address Translation (NAT) hides internal network structure from external threats. However, NAT can impact Quality of Service (QoS) in VoIP systems, causing increased latency and jitter, which may degrade voice quality.
4. Authentication and Access Control
   Strong authentication policies, including complex usernames and passwords and two-factor authentication, limit unauthorized system access. IP-based access controls ensure that only authorized devices can connect to the VoIP network. These measures are crucial to prevent misuse and maintain secure communications.

**E. Security Threats to VoIP Systems**

VoIP has transformed modern communication by offering efficient, internet-based voice services. However, its widespread adoption also exposes it to several security threats that jeopardize confidentiality, integrity, and availability. These threats include eavesdropping, Denial of Service (DoS) attacks, and spoofing.

1. Eavesdropping
   Eavesdropping is the unauthorized interception of VoIP conversations. Because VoIP transmits voice data over public networks, transmissions are vulnerable to interception if not properly encrypted. Without encryption, voice packets can be easily captured and analyzed by unauthorized parties, leading to sensitive information leaks such as business conversations or personal data, which can be exploited for identity theft or industrial espionage. End-to-end encryption using protocols like SRTP and TLS is strongly recommended to secure voice data. [13]
2. Denial of Service (DoS) Attacks
   DoS attacks aim to make VoIP services unavailable to legitimate users by overwhelming servers or networks with excessive traffic. This can cause service disruption, degraded call quality, or complete service outages. DoS attacks can involve sending invalid requests or flooding servers with high volumes of traffic. Effective detection and mitigation strategies include advanced firewalls, IDS, IPS, real-time traffic monitoring, and regular software updates.
3. Spoofing
   Spoofing in VoIP involves falsifying the caller's identity to commit fraud or gain unauthorized access. A common form is Caller ID spoofing, where attackers manipulate caller information to deceive recipients into revealing sensitive data or taking specific actions. For instance, an attacker may impersonate a bank or official institution to trick victims into disclosing account



https://doi.org/10.63876/ijss.v1i3.69

numbers or personal details. Preventing spoofing requires strong authentication mechanisms like the STIR/SHAKEN protocols, which verify caller identity authenticity. Users should also remain vigilant against suspicious calls and avoid sharing personal information with unknown callers.[1]

### F. Risk Identification in VoIP

Despite benefits such as cost efficiency and flexibility, VoIP systems are vulnerable to significant risks, mainly due to the open nature of IP networks and standard protocols like SIP and RTP, which do not provide strong encryption or authentication by default. VoIP systems often require firewall configurations that open specific ports, increasing the attack surface. Common risks include packet sniffing leading to eavesdropping, session hijacking, and targeted DoS attacks. Proper risk assessment is essential to design layered security frameworks that mitigate vulnerabilities and ensure secure voice communication over IP networks.

## METHODS

This study employs a literature review method by collecting, examining, and analyzing various relevant scholarly sources such as international journals, conference proceedings, technical articles, and standard documents related to the security of Voice over Internet Protocol (VoIP) systems. This method was selected to gain a comprehensive understanding of the common security threats encountered in VoIP implementations, as well as to identify strategies and solutions that can enhance system security.

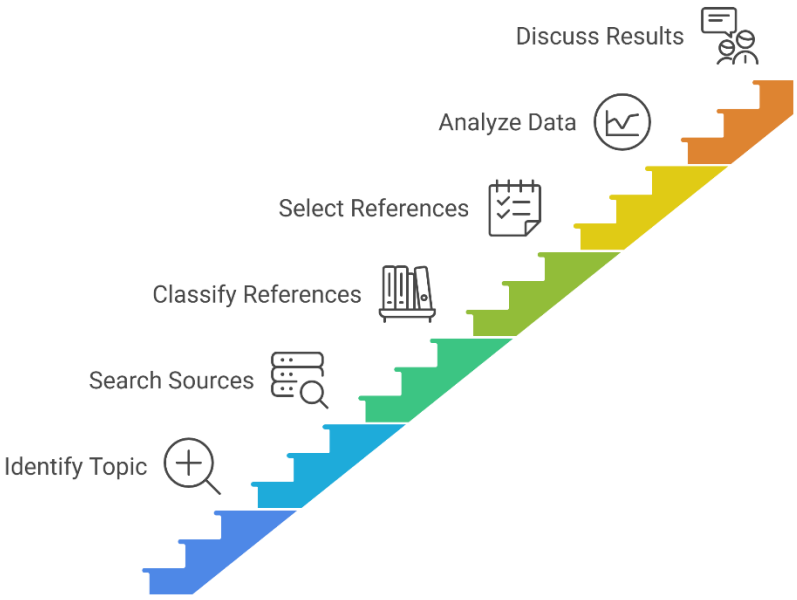


Figure 1. Enhancing VoIP Security

The research stages began with the identification of the main topic, focusing on VoIP security aspects. This was followed by a systematic search of scientific sources through databases such as IEEE Xplore, ScienceDirect, Google Scholar, and accredited national journals. Subsequently, the references were classified based on types of threats (e.g., eavesdropping, DoS, spoofing) and security approaches (e.g., encryption, firewalls, authentication).

The inclusion criteria for selecting references include:

1. Relevance to VoIP security systems,
2. Availability of data and technical information supporting the analysis.



https://doi.org/10.63876/ijss.v1i3.69

The collected data were then analyzed using descriptive-qualitative techniques to map out threat types, system vulnerabilities, and the effectiveness of security solutions based on previous studies. The results of this analysis served as the foundation for the discussion on the current state of VoIP security and its potential improvements.

## RESULT AND DISCUSSION

The results of this study indicate that Voice over Internet Protocol (VoIP) systems face significant security challenges that can threaten the confidentiality, integrity, and availability of voice communications. The open and complex architecture of VoIP, which includes components such as endpoints, SIP servers, media gateways, and public IP networks, makes it vulnerable to various types of attacks. Each of these components has its own vulnerabilities that need to be thoroughly identified and secured.

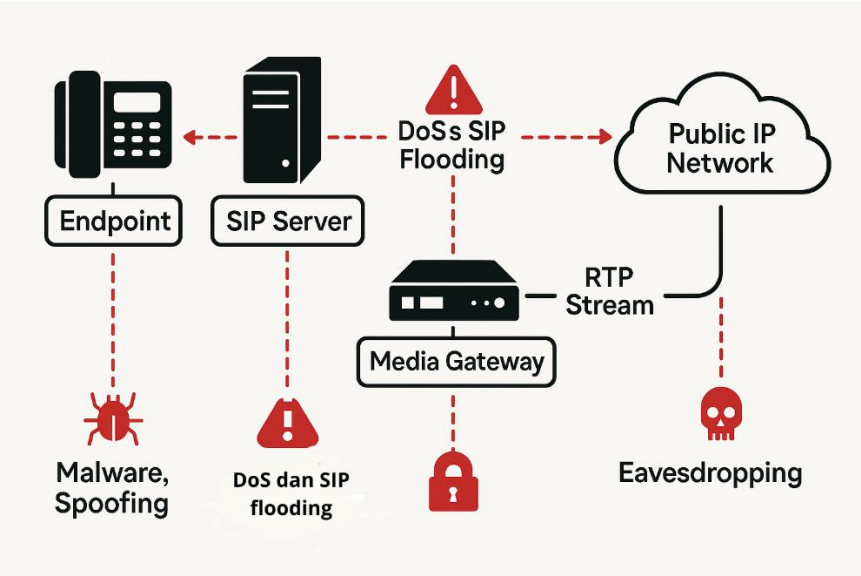


Figure 2. VoIP System Architecture and Vulnerability Points

Endpoints, such as IP phones or softphones, serve as the starting and ending points of VoIP communication. Since they are often directly connected to public networks, endpoints are susceptible to malware and spoofing attacks. Malware can infect devices, steal sensitive data, or even take control of the device. Spoofing allows attackers to impersonate legitimate users, commit fraud, or gain unauthorized access to the system. To mitigate these risks, it is important to implement strong authentication, regular software updates, and the use of secure endpoint devices.

The SIP server functions as the coordinator for initiating, maintaining, and terminating communication sessions. Due to its central role, the SIP server is a primary target for Denial of Service (DoS) and SIP flooding attacks. These attacks can overwhelm the server, causing it to become unresponsive or crash, thereby disrupting the overall communication service. To protect the SIP server, it is recommended to use application-layer firewalls, intrusion detection and prevention systems (IDS/IPS), and proper configuration to restrict unauthorized access.

The media gateway connects the VoIP network with traditional telephone networks (PSTN). If improperly configured, the gateway can be exploited for protocol manipulation attacks, such as call interception or redirection. To mitigate such risks, it is essential to ensure correct configuration, regular software updates, and the use of secure gateway devices.

RTP streams are used to transmit voice media during communication sessions. If RTP streams are not encrypted, voice data can be intercepted (eavesdropping), leading to leakage of sensitive information.



https://doi.org/10.63876/ijss.v1i3.69

To protect RTP streams, it is advised to use Secure RTP (SRTP), which provides encryption and authentication for RTP packets, as well as Transport Layer Security (TLS) to encrypt SIP signaling.

The security of VoIP systems does not rely solely on a single technical solution but requires a layered approach encompassing physical, application, and network protections. Each component in the VoIP architecture must be secured both individually and collectively to establish a robust defense against various threats. Implementing solutions such as firewalls, IDS/IPS, encryption, and strong authentication can significantly reduce the risk of attacks and ensure the continuity of communication services.

Table 1 Security Threat Analysis and Solutions in VoIP Systems

| **Security Threat** | **Attack Mechanism** | **Impact** | **Technology Solution** |
|---|---|---|---|
| Eavesdropping | RTP/SIP interception | Leakage of sensitive data | SRTP & TLS encryption |
| DoS | SIP server flooding | Service disruption, downtime | IDS/IPS, adaptive firewall |
| Spoofing | User identity forgery | Fraud, social engineering | STIR/SHAKEN, two-factor authentication |
| Session Hijacking | Active session interception | Unauthorized access, communication manipulation | Use of nonces and session tokens |
| NAT Traversal | Disruption in communication across NAT networks | Packet loss, degraded quality | STUN, TURN, ICE |

Table 1 explains various common security threats in VoIP systems, the attack mechanisms used, their impacts, and the technological solutions that can be applied to address them. The first and most frequent threat is eavesdropping on RTP and SIP data streams. This interception allows unauthorized parties to access sensitive information within voice communications, making data leakage highly likely. To counter this, encryption technologies such as Secure Real-time Transport Protocol (SRTP) and Transport Layer Security (TLS) are the primary effective solutions. SRTP encrypts voice packets, protecting communication content from interception, while TLS secures the SIP signaling that manages communication sessions.

The second significant threat is Denial of Service (DoS) attacks targeting SIP servers through flooding techniques. These attacks aim to render the server unresponsive, causing disruptions or even downtime in communication services. The impact of DoS attacks is critical as they can sever essential voice communications. To mitigate DoS attacks, the use of adaptive firewalls and intrusion detection and prevention systems (IDS/IPS) is strongly recommended. These technologies filter network traffic and block suspicious packets before they reach the main server.

Next is spoofing, which involves forging user identities in VoIP systems. Spoofing is often used to commit fraud or social engineering attacks that harm legitimate users. An effective solution to reduce spoofing risks is implementing the STIR/SHAKEN protocol, which provides dual authentication for the caller's identity, enabling detection and blocking of forged identities.

Another threat is session hijacking, where attackers intercept active communication sessions to illegally access and manipulate data. Prevention of this attack type can be achieved by using nonces and session tokens that act as unique keys for each communication session, minimizing unauthorized access.

Lastly, NAT traversal issues present challenges in VoIP communication across networks using Network Address Translation (NAT). These problems cause data packets to be lost or voice quality to degrade.



https://doi.org/10.63876/ijss.v1i3.69

Technical solutions such as STUN, TURN, and ICE enable communication to continue despite traversing complex NAT networks.[19]

However, the implementation of these security technologies often introduces additional challenges such as increased latency and jitter in communication. Intensive encryption and packet inspection require extra processing that can slow down real-time voice data transmission. Therefore, the implementation of security solutions must balance maintaining security with preserving quality of service (QoS) to ensure smooth and effective communication.

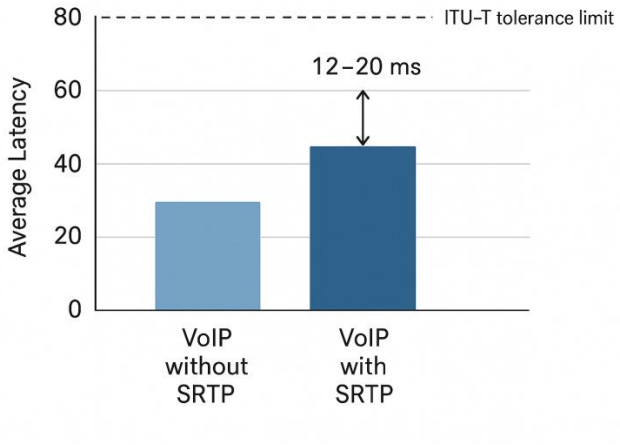


Figure 3. The Effect of SRTP Activation on VoIP Communication Latency

The implementation of the Secure Real-time Transport Protocol (SRTP) in Voice over Internet Protocol (VoIP) systems aims to enhance the security of voice communications through encryption and authentication. However, this encryption process requires additional processing time, which can impact communication latency. Figure 2 shows that enabling SRTP increases average latency by approximately 12 to 20 milliseconds compared to unencrypted VoIP communication.

Despite this increase in latency, according to ITU-T G.114 standards, it remains within the acceptable threshold for one-way end-to-end latency in real-time communication, which is a maximum of 150 milliseconds. In this context, an additional 12 to 20 milliseconds is considered acceptable and does not significantly affect conversation quality. However, it is important to consider that other factors such as jitter, network quality, and device configuration also influence the overall user experience.

Research by Asraf, Davies, and Grout (2009) indicates that SRTP usage can increase latency by 10 to 30 milliseconds per call, which may impact real-time communication. Nevertheless, they also note that SRTP is specifically designed for real-time applications, helping to minimize processing delays. Additionally, a study by Youk et al. (2007) emphasizes that while SRTP introduces additional latency, its impact on overall voice quality remains acceptable due to the enhanced security it provides.

Therefore, although the implementation of SRTP adds some latency to VoIP communication, the increase remains within internationally accepted limits, and the security benefits outweigh the minor performance impact. Nonetheless, to ensure optimal communication quality, it is essential to consider other factors such as network quality and device configuration when implementing SRTP.

Based on these findings, it can be concluded that the security of VoIP systems largely depends on the implementation of appropriate technical solutions and optimal system configurations. The deployment of application-layer firewalls and intrusion detection systems (IDS) has proven to be crucial in filtering SIP and RTP traffic, effectively preventing DoS and flooding attacks commonly targeting SIP servers. Additionally, end-to-end encryption using protocols such as Secure RTP (SRTP) and Transport Layer



https://doi.org/10.63876/ijss.v1i3.69

Security (TLS) not only ensures privacy protection but also proves effective in preventing eavesdropping and communication tampering, as supported by the study of Amor Lazzez (2013).

However, the primary weaknesses in VoIP security do not solely stem from the protocols themselves, but more often from suboptimal system configurations, which create vulnerabilities to attacks such as spoofing and session hijacking. Furthermore, although security protocols like STIR/SHAKEN can reduce the risk of user identity spoofing, their implementation remains limited due to infrastructure constraints among telecommunications operators. The use of VPNs for remote access also offers significant benefits for securing communication over open networks, although a balance with Quality of Service (QoS) policies is necessary to avoid degrading voice quality.

These overall findings highlight the importance of a layered security approach that combines encryption technologies, attack detection mechanisms, and robust system configuration to ensure both the security and service quality of VoIP systems.

## CONCLUSION

This study emphasizes that while Voice over Internet Protocol (VoIP) systems offer significant advantages such as cost savings, flexibility, and integration with digital services, they also face serious security challenges. The open architecture and reliance on public networks expose VoIP systems to threats like eavesdropping, Denial of Service (DoS) attacks, spoofing, and session hijacking. Implementing robust security measures including end-to-end encryption (SRTP and TLS), intrusion detection and prevention systems (IDS/IPS), adaptive firewalls, and strong authentication protocols such as STIR/SHAKEN is essential to safeguard the confidentiality, integrity, and availability of VoIP communications. Although these security solutions may introduce minor performance impacts such as increased latency, the trade-off is generally acceptable and necessary to maintain secure and reliable communication. Furthermore, the study highlights that the main weaknesses in VoIP security often arise not from the protocols themselves but from poor system configurations and inadequate infrastructure. Addressing these vulnerabilities requires a layered security strategy, combining technical protections with optimal system setup and continuous monitoring. Additionally, balancing security measures with Quality of Service (QoS) is crucial to ensure that enhanced protection does not degrade the user experience. Overall, the findings underscore the importance of comprehensive planning and implementation of security mechanisms to enable VoIP to continue evolving as a secure and efficient communication solution for the future.

## REFERENCES


[1] S. S. M. Saqquaf, P. Bhagyalakshmi, S. M. Shruti, B. M. Varsha, and S. Araballi, "Dynamically Automated Interactive Voice Response System for Smart city Surveillance," *2016 IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. RTEICT 2016 - Proc.*, pp. 1176–1180, 2017, doi: https://doi.org/10.1109/RTEICT.2016.7808017.

[2] P. Hoole and S. Hoole, *Lightning Engineering: Physics, Computer-based Test-bed, Protection of Ground and Airborne Systems*. 2022. doi: https://doi.org/10.1007/978-3-030-94728-6.

[3] A. M. Ramly, Z. W. Ng, Y. Khamayseh, C. S. C. Kwan, A. Amphawan, and T. K. Neo, "Review and Enhancement of VoIP Security: Identifying Vulnerabilities and Proposing Integrated Solutions," *J. Telecommun. Digit. Econ.*, vol. 12, no. 4, pp. 109–136, 2024, doi: https://doi.org/10.18080/jtde.v12n4.1022.

[4] M. M. Huda, *Keamanan Informasi*. 2020.

[5] J. Liang, S. Chen, Z. Wei, S. Zhao, and W. Zhao, "HAGDetector: Heterogeneous DGA domain name detection model," *Comput. Secur.*, vol. 120, p. 102803, Sep. 2022, doi: https://doi.org/10.1016/j.cose.2022.102803.

[6] C. Cuevas, R. Martínez, D. Berjón, and N. García, “Detection of Stationary Foreground Objects Using Multiple Nonparametric Background-Foreground Models on a Finite State Machine,” *IEEE Trans. Image Process.*, vol. 26, no. 3, 2016.

[7] H. Sinnreich and A. B. Johnston, *Using SIP Henry Sinnreich*. 2012.

[8] D. Stuttard and M. Pinto, *The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws*, vol. 7. 2011.

[9] R. Punna, G. Aravamuthan, and S. Kar, “Recovering 3D from 2D Image Points (Calibrated Camera Approach for Surveillance),” in *2022 IEEE 7th International conference for Convergence in Technology, I2CT 2022*, 2022. doi: https://doi.org/10.1109/I2CT54291.2022.9825444.

[10] D. Azizi and V. Arinal, “Sistem Monitoring Daya Listrik Menggunakan Internet of Thing (Iot) Berbasis Mobile,” *J. Indones. Manaj. Inform. dan Komun.*, vol. 4, no. 3, pp. 1808–1813, 2023, doi: https://doi.org/10.35870/jimik.v4i3.409.

[11] C. Chen, “Combining quality of services path first routing and admission control to support VoIP traffic,” *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1742–1750, 2013, doi: https://doi.org/10.1016/j.future.2012.03.026.

[12] F. D. Silalahi, “Keamanan Cyber (Cyber Security),” *Penerbit Yayasan Prima Agus Tek.*, pp. 1–285, 2022.

[13] J. Jokinen, T. Latvala, and J. L. M. Lastra, “Integrating smart city services using Arrowhead framework,” *IECON Proc. (Industrial Electron. Conf.*, pp. 5568–5573, 2016, doi: https://doi.org/10.1109/IECON.2016.7793708.

[14] H. Hsieh, J. Chen, A. Benslimane, and C. Applications, “5G Virtualized Multi-access Edge Computing Platform for IoT Applications,” 2018, doi: https://doi.org/10.1016/j.jnca.2018.05.001.This.

[15] A. Patil, S. Yadav, and M. Pandey, “Exploring Emerging Trends in AI-Driven Technological Advancements,” *Int. J. Technol. Model.*, vol. 3, no. 3, pp. 138–151, Dec. 2024, doi: https://doi.org/10.63876/ijtm.v3i3.140.

[16] A. V Savchenko, “Maximum-likelihood approximate nearest neighbor method in real- time image recognition,” *Pattern Recognit.*, vol. 61, pp. 459–469, 2017, doi: https://doi.org/10.1016/j.patcog.2016.08.015.

[17] T. M. Đức and N. T. Hương, “Improvement of Vehicle detection and classification performance with Region of Interest,” *ITEJ (Information Technol. Eng. Journals)*, vol. 8, no. 1, pp. 34–41, Jul. 2023, doi: https://doi.org/10.24235/itej.v8i1.116.

[18] K. Biswas and V. Muthukkumarasamy, “Securing smart cities using blockchain technology,” *Proc. - 18th IEEE Int. Conf. High Perform. Comput. Commun. 14th IEEE Int. Conf. Smart City 2nd IEEE Int. Conf. Data Sci. Syst. HPCC/SmartCity/DSS 2016*, pp. 1392–1393, 2017, doi: https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198.

[19] A. A. Simiscuka, “A Networking Scheme for an Internet of Things Integration Platform,” *2017 IEEE Int. Conf. Commun. Work. (ICC Work.*, pp. 271–276, 2017, doi: https://doi.org/10.1109/ICCW.2017.7962669.

[20] G. L. Foresti, L. Marcenaro, and C. S. Regazzoni, “Automatic detection and indexing of video-event shots for surveillance applications,” *IEEE Trans. Multimed.*, vol. 4, no. 4, pp. 459 – 471, 2002, doi: https://doi.org/10.1109/TMM.2002.802024.

[21] H. Badan and G. Indonesia, “Rancangan Pengem bangan Sistem Layanan Diseminasi Peringatan Dini Tsunam i Berbasis Service Oriented Architecture ( SOA ) ( Studi kasus :

Badan M eteorologi Klim atologi dan Geofisika ),” vol. 02, no. 03, pp. 230–243, 2019.

[22] S. T. Kouyoumdjieva, P. Danielis, and G. Karlsson, “Survey of Non-Image-Based Approaches for Counting People,” *IEEE Commun. Surv. Tutorials*, vol. 22, no. 2, pp. 1305–1336, 2020, doi: https://doi.org/10.1109/COMST.2019.2902824.

[23] F. Porikli, Y. Ivanov, and T. Haga, “Robust abandoned object detection using dual foregrounds,” *EURASIP J. Adv. Signal Process.*, vol. 2008, 2008, doi: https://doi.org/10.1155/2008/197875.



https://doi.org/10.63876/ijss.v1i3.69