Open Access Research Journal of
Science and Technology
Journals home page: https://oarjst.com/
ISSN: 2782-9960 (Online)

OARJ OPEN ACCESS RESEARCH JOURNALS

(REVIEW ARTICLE)

Towards resilient VoIP infrastructure: Identifying critical vulnerabilities and proposing unified security enhancements

Kelvin Ojanomare *

Technical Security Department, VOISIP Telecommunications Limited United Kingdom.

Open Access Research Journal of Science and Technology, 2025, 14(02), 175-192

Publication history: Received on 15 July 2025; revised on 26 August; accepted on 29 August 2025

Article DOI: https://doi.org/10.53022/oarjst.2025.14.2.0110

Abstract

Voice over Internet Protocol (VoIP) has transitioned from a novel technology to a cornerstone of organizational communication. However, the accelerated pace of VoIP adoption has amplified exposure to sophisticated security vulnerabilities. These vulnerabilities pose risks to confidentiality, availability, and integrity, and adversaries are increasingly targeting weaknesses in signaling protocols, media handling, device configurations, and network architectures. A unified, robust, and context-aware security model for VoIP is of great importance. This qualitative research paper delves into the existing vulnerabilities that continue to plague current VoIP infrastructures. Drawing from technical documentation, operational records, and security event analysis, the study provides an in-depth examination of vulnerabilities across different components of VoIP systems. The research also investigates recurrent patterns in VoIP security vulnerabilities, such as protocol weaknesses, misconfigurations, architectural inconsistencies, and inadequate policy enforcement. Moreover, it analyzes systemic factors that contribute to the persistence of these vulnerabilities across different organizations. Based on the insights gained, the study outlines a unified framework for security enhancements that focuses on strengthening architectural controls, harmonizing policy measures, and incorporating adaptive defense mechanisms. The results highlight that VoIP resilience cannot be solely achieved through isolated countermeasures but rather through a holistic, multilayered approach that collectively addresses technical, operational, and organizational gaps. This framework offers valuable contributions to the existing discourse by providing a unified pathway toward robust VoIP security, improved governance, and enhanced infrastructural resilience.

Keywords: VoIP Security; Network Resilience; Unified Security Framework; Protocol Vulnerabilities; SIP Security; Cybersecurity; Secure Telephony

1. Introduction

Voice over Internet Protocol (VoIP) has emerged as a ubiquitous communication platform deployed in corporate, government, and consumer settings. It enables the real-time transmission of audio, video, and messaging services over IP networks, offering a flexible and cost-effective alternative to traditional telephony (Fujifilm Business Innovation, 2020). VoIP has seen widespread adoption due to increased broadband capacity, cloud-based communication platforms, and rich-media collaboration technologies (Saenger et al, 2020). The transition of voice services to converged IP networks has placed VoIP at the forefront of digital transformation efforts, remote work enablement, and global communication strategies (Joachim et al, 2017).

The convergence on IP networks has exposed VoIP to an ever-widening scope of security risks. Unlike legacy circuit-switched telephony systems, VoIP is subject to the vulnerabilities inherent to IP networking, including eavesdropping, signaling attacks, session hijacking, and DoS (Wang and Chen, 2021). The complexity of VoIP protocols (e.g., SIP, RTP) coupled with inconsistent deployments and a mix of different devices compounds the attack surface (Younes and Umar,

* Corresponding author: Kelvin Ojanomare

Copyright © 2025 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0.

2022). As such, VoIP traffic has been found to be especially enticing to adversaries as it contains high-value, time-sensitive data and typically flows on networks that favor availability over security (Hossein et al, 2013)

While VoIP's dependence on IP networks necessitates constant improvements in encryption, authentication, segmentation, and intrusion detection, its infrastructures remain plagued by various problems of protocol fragility, misconfigurations, interoperability issues, and governance gaps (Ramly et al, 2024). To compound the matter, many existing deployments feature a disjointed set of security controls that fail to coalesce into a comprehensive defense strategy, leaving gaps in visibility and inconsistent threat responses (Alabdulatif et al., 2021). With VoIP infrastructures becoming more distributed (and more integrated with mobile devices, cloud services, and IoT endpoints), the industry requires VoIP-specific approaches to security that are resilient, harmonized, and multi-layered (Phithakkitnukoon and Weber, 2008).

This paper contributes to this emerging body of research by performing a qualitative analysis of the architectural and operational security vulnerabilities of today's VoIP infrastructures. By reviewing technical specifications, operational artifacts, and existing research publications, this study aims to surface recurrent themes of insecurity in VoIP and articulate these concepts in an integrated security enhancement model. The purpose is to connect the currently fragmented field of VoIP security into a more cohesive field that provides actionable guidance to security architects and VoIP engineers.

The value of this work is its integrative lens: VoIP's vulnerabilities are seldom treated as individual technical deficiencies but are instead understood as issues which permeate all aspects of the network stack, the operational policy, and configuration settings. The synthesis of all these dimensions into a single coherent research narrative is the primary focus of the paper and is expected to add to the cybersecurity literature by providing organizational decision-makers with a security-first understanding of VoIP.

2. Literature Review

2.1. VoIP Architecture and Communication Models

Voice over Internet Protocol (VoIP) technology refers to a set of methodologies and standards enabling the transmission of multimedia content, most often voice, across packet-switched Internet Protocol (IP) networks rather than through the circuit-switched infrastructure of the traditional Public Switched Telephone Network (PSTN). VoIP can be characterized by the processes of encoding, packetizing, transmitting, and decoding analog voice signals over IP networks (Ramly et al, 2024). In its classic form, a VoIP system consists of endpoints (softphones or IP phones), call control servers, media gateways, and a signaling protocol stack to establish, manage, and terminate sessions (Karapantazis and Pavlidou, 2009).

Session Initiation Protocol (SIP) is by far the most common signaling protocol due to its modular design and compatibility with various network infrastructures (Geneiatakis et al, 2005). Real-time Transport Protocol (RTP) provides a foundation for media delivery, while its encrypted counterpart Secure RTP (SRTP) can be used to encrypt voice traffic and prevent interception (Kuhn et al, 2005). Over time, the typical VoIP deployment environment has evolved to include cloud-hosted platforms, hybrid on-premises/cloud deployments, and mobile device integration, which has increased their complexity and correspondingly their operational and security requirements (Anwer et al., 2028).

2.2. Documented VoIP Vulnerabilities

Due to its reliance on open, unencrypted protocols, real-time data flows, and integration with heterogeneous networks, VoIP presents a multi-faceted attack surface for threat actors. Existing literature outlines vulnerabilities that can be broadly categorized as signaling manipulation, media interception, endpoint compromise, and network-layer exploitation (Dharmin and Parag, 2020).

SIP, as the most widely deployed signaling protocol, is vulnerable to spoofing, registration hijacking, replay attacks, and malformed message injection, among other issues, due to weak default authentication and the common use of plaintext (Akshay et al., 2014). Attackers may intercept SIP INVITE or REGISTER messages to gain information about sessions, or they may inject malicious BYE packets to disrupt active calls (Dassouki, 2017). Vulnerabilities at the media layer include RTP session hijacking, jitter buffer manipulation, and packet replay to facilitate the interception or tampering of audio streams (Baugher et al. 2004). Additionally, VoIP systems are susceptible to distributed denial-of-service (DDoS) attacks against SIP servers, which can degrade performance or cause total service disruptions (Nazih et al, 2020).

The critical assessment by Tuleun (2024) identifies a broad range of potential vulnerabilities in Asterisk-based VoIP systems and is oriented primarily around weaknesses in signaling controllers, media servers, device configuration, and authentication infrastructure, many of which are the result of simple misconfigurations and insecure default settings

In particular, Tuleun's review of the literature highlights how VoIP systems that are misconfigured, do not encrypt call and control traffic, and employ default passwords or run on unsegmented networks are most vulnerable to spoofing, session hijacking, eavesdropping, and other attacks.

The reviewed sources thus collectively suggest that the most common documented vulnerabilities in VoIP systems require coordinated, unified solutions.

2.3. Existing VoIP Security Solutions

Traditional VoIP security approaches have been built around the implementation of layered defense-in-depth mechanisms across signaling, media, and network layers. Encryption technologies like TLS for SIP signaling and SRTP for media streams can be used to secure data in transit against interception and tampering (Bugeja and Fibian, 2011). Authentication mechanisms, digital certificate-based trust models, and strong credential management can also help prevent impersonation and unauthorized access (Younes and Umar, 2022). Network segmentation and firewall-based VoIP filtering can help limit exposure and lateral movement of threats in the event of a compromise (Lee, 2008).

Intrusion detection systems (IDS) that are specifically designed for VoIP traffic analysis can be used to identify anomalous call patterns, brute-force registration attacks, and signaling irregularities (Vuong and Bai, 2004). Session border controllers (SBCs) are also often employed as policy enforcement points that can control the flow of traffic between different VoIP networks and provide topology hiding, media anchoring, and signaling protection (Francis et al. 2014).

However, many VoIP environments remain exposed due to the inconsistent adoption of security measures and misconfigurations or gaps in their deployment across teams and environments.

2.4. Existing Knowledge Gaps

While significant research effort has been invested in understanding individual vulnerabilities in VoIP systems and exploring isolated mitigation strategies, several key knowledge gaps have been identified. First, most individual vulnerability studies focus on threats to specific protocols (e.g., SIP flooding or RTP hijacking) without sufficiently considering interdependencies across architectural layers (Dantu et al., 2009). Likewise, most security models that have been developed for VoIP focus on technical controls, to the exclusion of key factors such as governance, configuration practices, or operational behavior (Jabra, 2020).

A key area where more research is needed is in exploring how and why security practices are often fragmented or poorly coordinated across enterprises. Many companies still deploy VoIP systems with collections of security tools (firewalls, VPNs, encryption) but do not have integrated monitoring or baseline configurations across these settings (Angelos, 2010). As a result, these individual security functions are often unable to provide broad protection against multi-vector attacks.

The assessment by Tuleun (2024) supports this conclusion and in particular finds that even when individual VoIP security controls are correctly applied, they often fail because of inconsistencies across devices, incomplete implementation, or failure to keep authentication and encryption practices up to date

These results point to a need for unified, cross-cutting security frameworks that can effectively coordinate policy, configuration, and security operations.

Another gap is a lack of in-depth qualitative research on the experiences, challenges, and real-world considerations that practitioners face in VoIP security implementation. Addressing this gap is one of the primary goals of this study.

2.5. Summary of Key Literature Findings

The reviewed literature suggests that while VoIP technology provides robust communication functionality, it remains intrinsically vulnerable to threats resulting from its protocol design, architectural complexity, and operational inconsistencies. Although numerous security controls are available, they are commonly implemented in isolation,

limiting their ability to provide a comprehensive mitigation approach. This literature review thus lays the foundation for the development of a unified, multilayered security enhancement framework, which is the objective of this research.

3. Research Methodology

3.1. Research Design

The design of this research will be based on a qualitative study which seeks to understand the issues as they are. The reason for adopting a qualitative study design is to capture the complex nature of operational environments, and the vulnerabilities are all a function of the operating environments which cannot be numerically represented (Flick, 2018). Security failures in VoIP also tend to be the result of interactions of several causal factors that may be technical, operational, and process failures. In addition, as some of the weaknesses that were discovered may be transient or systemic, it is important to understand how they are manifested in practical deployments, which a qualitative and interpretative study design can accomplish.

The study will be document-based, meaning that the work will gather, review, and synthesize information from VoIP documentation and system configuration files, security incident reports, and VoIP-related research to identify vulnerabilities and behavioral patterns. The review will also consider theoretical vulnerabilities from academic studies and technical reviews and vulnerabilities and attack patterns that have been reported in operational contexts. The data analysis will follow a process of content analysis.

3.2. Sources of Data

The primary source of data for this study is from documented materials such as

- VoIP Technical documentation (RFCs, specification documents, vendor documents)
- Network configuration and log files (SIP network topologies, dial plan files, firewall configurations, et al.)
- Security event logs, security event reports
- Articles and Journals on VoIP vulnerabilities and design security considerations
- Security white papers, advisories, and security updates
- VoIP Deployment and configuration guides

A very important source of data is the VoIP Deployment and Security Analysis work by Tuleun (2024), which offers a comprehensive case study on the design, deployment, and use of an Asterisk-based VoIP system (Tuleun, 2024). A variety of deployment and security considerations are discussed in the report and where detailed information about security and potential security loopholes that could be utilized by adversaries is available. One of the reasons to choose the work as a key functional baseline is because of how specific information on the design can be useful in this study, specifically because it offers contextual considerations on aspects of VoIP design such as default configuration files and network design.

Studies that are qualitative allow for a review of the available materials to be able to triangulate information from all of the available documents to offer perspectives that may not have been derived when only considering one document.

3.3. Data Collection Strategy

The method for collecting the data was based on an orderly document collection and review process that was consistent with content analysis procedures recommended for qualitative studies. Documents that would be appropriate for VoIP studies were identified on the basis of focus on VoIP architecture, protocol behavior, and security. Bowen (2009) outlined several processes for documentary research, which were used to guide data collection in this research work. They include

- Identify: Possible sources of documentary information were identified through database searches, web-based libraries, and collection of publicly accessible VoIP Configuration files.
- Screen: The documents were then assessed on the basis of credibility, currency, and relevance to the selected topics.
- Catalog: Identified material was then grouped into topics for retrieval, which are based on major themes (such as signaling vulnerabilities, encryption practices, and organizational/systemic considerations).
- Iterative Review: Documents were then reviewed, which informed the refinement of themes as the review progressed.

The procedure above is consistent with qualitative research methods which focus on the production of narrative (Bowen, 2009). These sources of data provide a range of narrative data that may be authoritative, and diverse sources which can speak to both theoretical and operational dimensions of VoIP.

3.4. Data Analysis Procedures

The research work used thematic content analysis as its data analysis procedure. Content analysis of documents and written information is a well-established data analysis method that has proven suitable for pattern identification in qualitative datasets (Nowell et al., 2017). The following were the processes of analysis.

- Familiarization: Repeated reading of the identified documents.
- Coding: Open Coding of information and Concepts relevant to identifying VoIP vulnerabilities, architectural frailties, configuration errors, and security best practices
- Theme Identification: Identification of themes from the codes obtained during the coding phase which in this work are as follows:
- Patterns of Protocol-level vulnerabilities
- Patterns of exposure points at the network-layer
- Patterns of inconsistencies in VoIP configurations that could be termed as organizational-level inconsistencies.
- Patterns of fragmentation of existing security controls
- Integrative Interpretation: Themes were compared across documents to identify commonalities and divergences, offering a multi-perspective view of VoIP vulnerability ecosystems.

The process above has also been found to be consistent with the content analysis of text as it facilitates the production of information as narrative information (Bowen, 2009). The approach is not restricted to a specific data analysis procedure but can be applied to various texts.

3.5. Ethical Issues

The study does not capture any information from identifiable sources such as organizations. All the data used for this work is publicly available or are openly available information that is released and made available by authorization. This means that the study has not collected confidential information or proprietary information in its processes. The documents were screened to ensure they were credible and do not have any personally identifiable information (PII). The study is also cognizant of ethical considerations of secondary data analysis and ensure that all documents are reviewed in line with guidance on ethics in secondary data analysis, and use of the reviewed documents is carried out within the agreed-upon ethical boundaries (Macnish and Jeroen 2020).

Disclosure of information such as network configurations of the researched organization would not be included, and where parameters from the studied sources such as configuration files or VoIP log files are included, no specific configuration will be included that could be useful in causing harm.

4. Findings

The results of the qualitative study provided an insight into the multifaceted landscape of VoIP security. The interconnected themes, as identified in the analysis, unveiled a complex narrative where vulnerabilities in VoIP ecosystems are products of protocol deficiencies, architectural oversights, misconfigurations, and operational discrepancies. The findings have been synthesized into three overarching thematic categories, namely: (1) inherent technical vulnerabilities, (2) operational and organizational challenges, and (3) emerging patterns of threats and attack vectors.

4.1. Core Vulnerability Themes

4.1.1. Protocol and Encryption Gaps

An emergent theme from the findings was the existence of protocol and encryption gaps, particularly in the SIP and RTP protocols that are foundational to VoIP communications. The observed documentation of vulnerabilities and real-world exploits in the reviewed sources highlight the consequence of these gaps. The frequent use of plaintext transmission in SIP for initiation and control information surfaces as a consistent issue, which, when not addressed by using TLS, exposes the protocol to interception, modification, and spoofing attacks (Sven and Thomas, 2010). Similarly, the RTP streams, responsible for the actual media transfer, are found to be susceptible to hijacking and eavesdropping when not secured by SRTP (Session Initiation Protocol Secure).

The critical takeaway from this theme, as supported by the document analysis, is the elevated risk profile of VoIP systems that are not aligned with secure configuration best practices, particularly in SIP/RTP deployments (Tuleun, 2024). Misconfigurations, such as weak or absent authentication, unencrypted RTP streams, and open management interfaces, are often pointed out as clear enablers of call hijacking, message spoofing, and media interception (Tuleun, 2024). This finding dovetails with the broader observation from the data that protocol weaknesses become exponentially more perilous when they are not mitigated through careful configuration.

4.1.2. Endpoint and Device Security Concerns

Endpoints, including IP phones, softphones, mobile VoIP applications, and devices with embedded SIP capabilities, were identified as potential vulnerabilities. The focus on these components is substantiated by the instances of weak firmware, default passwords, unsecured web interfaces, and open provisioning services being targeted in the literature and case studies (Seeking et al, 2013). The threat actors leverage these weaknesses to

- Redirect calls to malicious endpoints;
- Tamper with dial plans;
- Capture SIP authentication credentials;
- Use compromised devices as a foothold for further attacks

As illustrated, these endpoints are not only entry points but can also serve as pivot points within an organization's network.

Furthermore, the analysis notes a theme of interoperability vulnerabilities arising from the interaction of devices from different vendors, leading to inconsistent parsing and processing of SIP messages. Attackers exploit these inconsistencies by crafting and injecting malformed SIP requests.

4.1.3. Network-Level Exposure Points

Network-level exposures were consistently seen in VoIP implementations that lack adequate segmentation, as highlighted by the findings. Weaknesses such as exposed SIP ports to public-facing networks, improperly configured firewall/NAT traversal rules, and unrestricted VLANs were common (NIST SP 800-58, 2005). The data pointed out a lack of topology obfuscation through Session Border Controllers (SBCs) as a recurring theme, creating a clear pathway for packet sniffing and call tampering.

Special attention is drawn to cloud-hosted VoIP environments, where the convergence of traditional networks with virtualized infrastructure presents new challenges. The findings here suggest a misalignment of trust boundaries and excessive permissions when on-premises VoIP traffic is extended to cloud-based PBXs without strict controls (Qubeb and Paramasivam, 2019).

4.2. Operational and Organizational Challenges

4.2.1. Fragmented Security Implementation

The qualitative data reflects a tendency towards fragmented or piecemeal security measures, with controls being implemented in isolation rather than as part of a holistic security strategy. The documents and articles show examples where encryption is applied inconsistently, such as using SIP-TLS without SRTP or deploying SBCs without an integrated Intrusion Detection System (IDS) (Ranganathan and Babu, 2020). This piecemeal approach leads to security gaps or "seams" that attackers can exploit, as they circumvent the weakest link in the security chain.

4.2.2. Misconfiguration as a Recurring Root Cause

Misconfiguration as a root cause of vulnerabilities and security incidents in VoIP systems is a recurring finding in the research. Inadequate or weak SIP authentication, overly permissive firewall rules, exposed management interfaces, and NAT/SIP ALG misalignments are documented as common errors that lead to security breaches (Nuno et al, 2020). The scholarly articles reviewed corroborate this by quantifying misconfigurations as contributing to more than half of all VoIP-related security incidents and performance issues.

4.2.3. Skills Gaps and Resource Limitations

A significant organizational challenge related to VoIP security is the shortage of skills and resources required for its administration. VoIP management demands specialized knowledge, which the findings note is often lacking in

organizations. The implications of this, as derived from both the documents and academic sources, include an overreliance on default configurations, incomplete security posture, and challenges in scaling and securing integrations with other systems (Fukuyama and Fujimoto, 2016).

4.3. Emerging Threat Patterns in Modern VoIP Ecosystems

4.3.1. Increasing Sophistication of Attack Chains

Complex and sophisticated attack patterns, involving multiple steps and interactions with the VoIP infrastructure, are an emerging trend in the threat landscape. As per the findings, these patterns include reconnaissance, SIP enumeration, brute-force attacks on credentials, and media-layer manipulation (Hasib et al, 2010). Attackers use these methods to:

- Probe for vulnerable SIP extensions;
- Execute targeted password attacks;
- Capture RTP streams;
- Inject malicious SIP BYE messages to terminate calls;

The methodical nature of these attack chains reflects an evolution towards more structured and strategic exploitation efforts.

4.3.2. VoIP Threats in Cloud and Hybrid Infrastructures

The shift to cloud and hybrid infrastructures has brought about specific security considerations, particularly around misconfiguration risks in cloud-hosted VoIP services. The qualitative data highlighted issues such as lax API access controls, poorly restricted IAM roles, insecure routing between virtual private clouds (VPCs), and misconfigured SBCs in cloud environments (Ezzah et al, 2024). Hybrid configurations, which mix on-premises and cloud-based components, exacerbate these risks due to often inconsistent security policies across environments.

4.3.3. VoIP Integration with IoT and Mobile Endpoints

The integration of mobile applications and IoT devices with VoIP services has expanded the threat surface. Mobile applications are particularly vulnerable to:

- Operating system (OS) compromises;
- Connections over unsecured or rogue Wi-Fi networks;
- Installation of malicious applications;
- Credential harvesting on the device itself (Azfar et al, 2016).

IoT devices that are SIP-enabled, such as smart intercoms or cameras, frequently have weak security mechanisms, making them relatively easy targets for attackers to penetrate VoIP networks.

4.4. Summary of Findings

The synthesis of findings from the qualitative content analysis of VoIP security challenges, as presented in various documents, illuminates the complex and layered nature of the ecosystem's vulnerabilities. It is evident that the issues are not only technical but also organizational and procedural. The insights gained underscore the critical importance of a comprehensive and unified approach to VoIP security, one that integrates multiple layers of defense to mitigate a wide range of risks. The data supports a strong argument for the development and implementation of a robust, multilayered, and cohesive VoIP security strategy that can address the full spectrum of threats.

5. Discussion

The patterns and trends revealed in the research findings indicate that VoIP infrastructures are vulnerable due to an array of technical, operational, and organizational factors. The present discussion section interprets those patterns and shows their relationship with the existing literature on VoIP resilience and reliability. Specifically, the fragmented state of VoIP security, protocol and interoperability weaknesses, and new directions for emerging attack surfaces are discussed in this context.

5.1. Interpretation of Key Patterns

5.1.1. VoIP Vulnerabilities Are Multifactorial and Interrelated

The main lesson from the research findings is that no VoIP vulnerability is isolated. A protocol weakness is more likely to be exploited when accompanied by network misconfigurations, lack of access control, or uneven security controls. This finding is not novel but complements existing literature on the trend toward multi-stage, multi-vector attack chains, which is becoming increasingly popular in attack frameworks targeting converged infrastructures (Wu et al, 2009).

For instance, inherent SIP and RTP vulnerabilities become operational when network or application-layer TLS/SRTP is inconsistently applied or when vulnerable VoIP endpoints are configured with default credentials. The key takeaway from the qualitative analysis of the results is that the majority of VoIP security breaches are due to the confluence of such weaknesses, rather than a single point of failure.

5.1.2. Configuration Governance Is Critical for VoIP Security

The role of misconfiguration in VoIP insecurity is also clearly indicated in the research findings and corroborates a common industry concern in this regard (Carrillo-Mudejar et al, 2022). In contrast to traditional telephony, which was more reliant on circuit switching, VoIP security highly depends on correct mapping between application-layer protocol hardening, network-layer control, and device-level settings. In this architecture, a wide range of small misconfigurations—such as incorrect SIP headers, missing MIME types, or relaxed firewall rules—can introduce significant attack surfaces.

The related literature review of the findings indicates that the VoIP community underestimates the complexity of the VoIP configuration and access control landscape. While best practices and tools such as SBCs, VPN, firewall, IDS/IPS, and DDoS protection are well-known and available, their success in mitigating security threats to VoIP infrastructure is closely linked to how they are consistently applied, if at all. This is in line with recent research showing that technical security measures are often undermined by operational inefficiencies (Kermit's, 2010).

5.1.3. Resource and Skill Constraints

Administrator expertise, or lack thereof, is another theme that is consistently observed across the data. As VoIP security operates at the intersection of telecommunications principles, IP networking, and cybersecurity, the community in charge of managing these systems must be knowledgeable about all three fields. This is borne out by international research that consistently lists VoIP and UC security expertise as one of the most in-demand and least available in enterprise cybersecurity operations (Alsebai and Abdrabbuh, 2021).

Consequently, many VoIP administrators rely on default settings for end devices, incomplete security policy application, or procrastinate when it comes to applying the latest patches.

5.2. Implications for Infrastructure Resilience

5.2.1. Integration and Alignment of Security Controls Is Necessary for VoIP Resilience

The overall finding from the data analysis is that security measures for VoIP are often applied in a piecemeal and disjointed manner, leading to critical gaps. This is one of the major factors influencing the resilience of such architectures. In other words, rather than the current state of defense-in-depth where mitigations are applied one by one without any integration, a holistic and unifying security framework for VoIP infrastructures is required.

Such an architecture should integrate and align a number of controls, such as

- Protocol hardening
- Network segmentation
- Encryption enforcement
- Endpoint hardening
- Continuous monitoring
- Administrative policy harmonization

This is highly consistent with recent research on resilience in cybersecurity, which calls for more coordinated and cross-layered defenses to effectively prevent cascading failures in converged network environments, such as telephony (Dantu, 2009).

5.2.2. Adaptive and Continuous Monitoring Is Required to Support Resilience

Continuous rather than static security controls are needed to support resilience. This is driven by the fact that VoIP is quickly evolving due to the shift toward the cloud, mobile softphones, and connected devices, especially those based on SIP. Attackers quickly adapted to all this as well by applying dynamic reconnaissance methods, protocol fuzzing, and credential brute-forcing, which require more adaptive mitigation measures, such as:

- IDS for VoIP based on anomaly detection
- Machine learning-based SIP traffic analysis
- Continuous monitoring and verification of endpoint security state (Alioto's et al, 2016).

5.2.3. Organizational Governance and Documentation Are Crucial

The research findings also suggest that appropriate governance is critical. In its absence, well-designed and VoIP-friendly infrastructure architecture is useless. Some of the top consequences of governance-related organizational issues, seen both in the data analysis and in other studies, include:

- Irregular use of encryption and other security-enhancing protocols.
- Untracked changes in firewall and network rules
- Forgotten, unprotected provisioning accounts and other administrative entry points.
- Policy drift and weaker policy compliance.

It is shown that maturity in governance, configuration documentation, change control, and standardization are directly related to higher security posture levels in converged network architectures, including VoIP systems (Valarie et al, 2010).

5.3. Alignment with Prior Research

The evidence presented in the study clearly aligns with the prior body of research and expands on it. The VoIP security community has long observed and lamented the lack of unified adoption of security measures and has singled out misconfiguration as a recurring issue in this ecosystem (Younes and Umar, 2022). The present study supports those observations while demonstrating that the underlying reasons often include more structural causes, such as resource and skill shortage, inconsistent governance, and lack of integration across security layers.

In addition, some prior research on cloud-based and hybrid VoIP deployment models, which is an ongoing trend, presaged significant expansion of the VoIP attack surface associated with the presence of multiple trust boundaries and misaligned policies (Ezzah et al, 2024). The evidence from this study provides support for those claims with regard to overlapping security controls and gaps at SIP servers, cloud APIs, and mobile and wireless VoIP endpoints.

Finally, the recognition of the role of multi-vector attack chains complements research on VoIP convergence-related security indicating that such exploits increasingly resemble coordinated cyberattacks reported in other real-time infrastructures (Ramly et al, 2024). It means that the same unified, non-traditional defense approaches may be required.

5.4. Summary of Discussion

In summary, the discussion section of the present report on insecure VoIP infrastructure has indicated that such issues are not due to one layer of infrastructure, one protocol, or one type of misconfiguration. Instead, the state of insecurity is observed due to an accumulation of vulnerabilities across an entire ecosystem composed of multiple interconnected services, a variety of heterogeneous devices, and new deployment patterns. It is precisely these insights that provide a direct link to the next section of the report, which outlines a unified security enhancement framework for modern VoIP.

6. Suggested Universal Security Solutions

In light of the VoIP vulnerabilities and operational gaps detailed above, I suggest a holistic, unified security architecture that combines technical, organizational, and procedural controls. VoIP security can be achieved not with a disparate set of ad-hoc countermeasures, but by a multilayered model that enforces consistency, monitoring, and resilience. This

section presents a unified security solution framework built on four core layers: (1) protocol and application hardening, (2) network and infrastructure security, (3) endpoint and device governance, and (4) security management and monitoring.

6.1. Protocol and Application Layer Hardening

6.1.1. Enforce Encryption for Signaling and Media

Unified security mandates encryption for all signaling and media data. Implement the following

- TLS for SIP signaling
- SRTP for voice media streams
- Certificate-based mutual authentication
- Disallow fallback to plaintext or weak ciphers

Research highlights that consistent SRTP/TLS deployment significantly improves confidentiality and integrity, reducing interception and manipulation risks (Bugeja and Fabian, 2011).

6.1.2. Implement Strong SIP Registration and Authentication Policies

- To thwart SIP spoofing, registration hijacking, and brute force attacks, I recommend the following controls
- Digest authentication with strong hashing algorithms
- Multi-factor authentication (MFA) where possible
- Rate limiting for SIP registration attempts
- SIP "fail2ban"-style intrusion blocking features

These controls will together minimize the risk of unauthorized access and help prevent credential compromise (Hasib et al, 2010).

6.1.3. Validate Protocol Behavior

Protocol fuzzing and malformed packet defense mechanisms should be implemented into SIP servers and SBCs. I propose systems should validate SIP headers, reject unexpected message formats, and sanitize message payloads to help prevent injection or teardown spoofing attacks.

Protocol validation is also supported by research that shows reduced incidents of call-flow manipulation attacks (Dasuki, 2017).

6.2. Network and Infrastructure Security

6.2.1. Isolate and Segment VoIP Traffic

VoIP systems should run on dedicated VLANs or isolated network segments to prevent lateral movement and packet sniffing. This minimizes exposure by ensuring VoIP packets never mix with general data traffic.

Network segmentation is one of the most effective countermeasures against VoIP-based reconnaissance and interception according to research (NIST SP 800-58, 2005).

6.2.2. Deploy and Configure Session Border Controllers (SBCs)

SBCs act as policy enforcement points to protect the VoIP perimeter. They should be deployed to

- Hide internal network topology
- Enforce signaling/media security policies
- Mitigate SIP DoS/DDoS attacks
- Normalize SIP messages and filter for malicious content

SBC deployment has also been strongly correlated with VoIP resilience in research (Francis et al. 2014).

6.2.3. Use Secure Tunnels for Inter-Site VoIP

Organizations running VoIP systems across multi-branch deployments must use site-to-site encrypted tunnels (IPSec or TLS-based VPNs) to protect traffic moving between untrusted networks.

Tuleun (2024) shows the need for this in practice, demonstrating how IPSec tunneling in Asterisk-based VoIP infrastructures mitigates eavesdropping, packet manipulation, and interception attacks across distributed network sites (Tuleun, 2024)

The paper provides a good practical demonstration of the necessity for encrypted tunnels as part of VoIP resilience.

6.3. Endpoint and Device Governance

6.3.1. Secure Provisioning and Endpoint Hardening

- Endpoints should be hardened with the following measures
- Disabled unused services and open ports
- Secure auto-provisioning (HTTPS, encrypted XML)
- Changed default passwords
- Enforced firmware updates

Endpoint compromise is also one of the most common VoIP attack methods, so device governance is critical (Seokung et al, 2013).

6.3.2. Mobile and IoT Endpoint Security

With the widespread adoption of mobile softphones and IoT SIP devices, the following controls are suggested

- Require encrypted connections (SRTP/TLS)
- Enforce mobile device management (MDM) policies
- Restrict VoIP access on untrusted networks
- Validate application integrity through secure app stores

Mobile VoIP adversaries are known to frequently exploit weak Wi-Fi security and outdated operating systems (Azfar et al, 2016), so these controls are crucial.

6.4. Security Monitoring and Management

6.4.1. Centralized Logging and Real-Time Monitoring

Unified VoIP security requires centralized collection and real-time monitoring of the following logs and statistics

- SIP logs
- RTP statistics
- SBC event alerts
- Firewall and IDS activity
- Authentication and registration events

Machine learning (ML) based traffic analysis can also detect anomalous patterns, such as rapid-fire registration attempts, anomalous jitter values, or unexpected call flows (He and Chen, 2023).

6.4.2. Intrusion Detection and Anomaly-Based Systems

VoIP-specific IDS solutions should be employed to monitor the following

- SIP message anomalies
- RTP injection attempts
- Protocol inconsistency
- DoS attack patterns

Such systems should be integrated into SIEM platforms for automated alerting and correlation.

6.4.3. Governance, Compliance, and Policy Alignment

Enforce consistency with unified governance across

- Configuration baselines
- Access control policies
- Patch/update schedules
- Change management procedures

Governance maturity has a direct correlation with VoIP resilience, as well-researched controls aligned with business needs stay enforced (Kim and Lee, 2021).

6.5. Proposed Framework Summary

The universal VoIP security model unifies the following

- Encryption and protocol hardening controls
- Network segmentation and SBC deployment
- Endpoint/device governance and hardening
- Continuous monitoring and security analytics
- Organizational governance and configuration management

In summary, this approach ensures VoIP security is not reliant on isolated controls but instead on coordinated, complementary layers that together build modern threat resilience.

7. Unified VoIP Security Framework

Synthesizing the vulnerabilities and proposed controls, this section presents a Unified VoIP Security Framework (UVSF) to provide a comprehensive, coordinated, and multilayered defense for contemporary VoIP environments. The UVSF unifies technical and organizational controls into a cohesive architecture, defined by five pillars: (1) Protocol Integrity and Encryption, (2) Network Segmentation and Perimeter Control, (3) Endpoint and Identity Governance, (4) Continuous Monitoring and Analytics, and (5) Governance and Compliance Alignment.

7.1. Pillar One: Protocol Integrity and Encryption

7.1.1. Mandatory SIP-TLS and SRTP Enforcement

VoIP environments should mandate strong encryption for all signaling and media traffic. This requires

- SIP over TLS with certificate validation
- SRTP for media encryption
- Rejection of insecure cipher suites

Mandatory encryption lowers the attack surface for eavesdropping and tampering (Bugeja and Fabian, 2011).

7.1.2. Protocol Validation and Normalization

To block SIP spoofing, malformed messages, and teardown manipulation, SBCs and SIP proxies should:

- Normalize SIP headers
- Enforce strict message formatting
- Apply rate limiting
- Filter anomalies

This closes the attack surface for protocol abuse (Dassouki, 2017).

7.1.3. Authentication Strengthening

- Robust SIP authentication mechanisms include
- Digest authentication with secure hashing

- MFA for administrative access
- Protection against brute-force attacks

Research shows strong authentication dramatically reduces the risk of unauthorized registrations (Hasib et al, 2010).

7.2. Pillar Two: Network Segmentation and Perimeter Control

7.2.1. VoIP Network Isolation

VoIP traffic should be network-isolated using

- VLAN segmentation
- Layer-3 isolation
- Strict ACLs

Segmentation minimizes the risk of sniffing attacks and lateral movement (NIST SP 800-58, 2005).

7.2.2. SBCs as Perimeter Defense

SBCs provide important controls, such as

- Topology hiding
- Media anchoring
- SIP DoS/DDoS filtering
- Protocol normalization

SBCs are critical in distributed, cloud-connected VoIP deployments (Francis et al. 2014).

7.2.3. Encrypted Inter-Site Tunnels

Site-to-site communication should use encrypted tunnels, e.g., IPSec, or TLS VPNs.

Tulum (2024) illustrates how incorrect or absent tunnel configurations in real-world Asterisk deployments can leave call traffic exposed to interception and manipulation, making a strong case for the need for enforced encrypted inter-site VoIP tunnels (Tulum, 2024) .

This empirical finding strongly supports encrypted tunneling as an essential part of VoIP perimeter defense.

7.3. Pillar Three: Endpoint and Identity Governance

7.3.1. Secure Provisioning and Hardening

- Endpoints must be hardened with
- Encrypted auto-provisioning
- Firmware updates
- Removal of default credentials
- Disabling of unused services

These steps are necessary to prevent endpoint takeover (Seokung et al, 2013).

7.3.2. Identity and Access Controls

unified identity approach requires

- RBAC for VoIP admin portals
- Credential rotation
- MFA for sensitive actions
- Managed identity stores

Identity governance enforcement greatly lowers the risk of impersonation and registration fraud (Azfar et al, 2016).

7.3.3. Mobile and IoT Endpoint Security

As softphones and IoT SIP devices become common, organizations must require:

- MDM controls
- Strong wireless security
- Application integrity checks

This secures mobile VoIP flows from OS-level compromise.

7.4. Pillar Four: Continuous Monitoring and Analytics

7.4.1. Specialized VoIP IDS/IPS Integration

VoIP-specific IDS solutions should be used to monitor:

- SIP registration anomalies
- RTP packet irregularities
- Malicious SIP flooding

These tools are needed to detect advanced VoIP attack chains (He and Chen, 2023).

7.4.2. Machine Learning–Driven Analytics

ML-based monitoring uncovers

- Suspicious calling behavior
- Unusual extension usage
- Rising registration failures
- Traffic anomalies in hybrid VoIP

Behavioral analysis can significantly improve early detection of targeted attacks.

7.4.3. Centralized Logging and Telemetry

Logs from SIP servers, SBCs, firewalls, routers, and endpoints must be collected into a SIEM for

- Correlation
- Threat hunting
- Incident reconstruction
- Compliance checks

Centralized telemetry dramatically improves situational awareness.

7.5. Pillar Five: Governance, Compliance, and Policy Alignment

Configuration Governance

Policy-aligned configuration baselines ensure the consistent application of:

- Encryption defaults
- SIP header rules
- Firewall/NAT policies
- Credential standards

Configuration governance drastically lowers the risk of misconfigurations, the leading cause of VoIP breaches (Carrillo-Mondéjar et al, 2022).

7.6. Administrator Competency and Training

- The UVSF assumes ongoing training for administrators in

- SIP/RTP protocol fundamentals
- VoIP security hardening
- Incident response for VoIP attacks
- Cloud PBX platforms

Skilled administrators are needed to support good technical controls.

7.6.1. Regulatory Compliance Alignment

VoIP systems should be aligned with

- GDPR
- HIPAA (if applicable)
- PCI-DSS
- ISO/IEC 27001

Compliance integration can help with both legal integrity and security.

7.7. Summary of Unified Framework

- The Unified VoIP Security Framework integrates all of the following
- End-to-end protocol encryption
- Network segmentation with a full SBC perimeter defense
- Hardened endpoints governed by strong IAM
- Continuous monitoring with VoIP-aware analytics
- Configuration governance and policy alignment

The unified model directly addresses fragmented defenses that are common in VoIP deployments by offering a coherent, multilayered security architecture that is designed to defend against modern VoIP cyber threats.

8. Conclusion

In conclusion, this study sought to consolidate and extend the existing knowledge around VoIP security issues by identifying and discussing persistent vulnerabilities within modern VoIP ecosystems. The results confirmed the study's hypothesis that these vulnerabilities are not isolated weaknesses but arise from a complex interplay of protocol design challenges, network exposure, endpoint governance, and organizational limitations. This finding supports the complexity of securing a real-time communications system that is distributed, open, and interoperable by design.

The qualitative analysis helped confirm that the intrinsic design limitations in SIP and RTP – along with implementation gaps in areas like incomplete or faulty encryption – remain the initial, and sometimes final, vector of exploitation for attackers. The findings also indicate that network layer weaknesses such as lack of segmentation and firewall/NAT traversal misconfigurations further exacerbate the risk, while endpoint devices continue to present soft targets through exposed interfaces, outdated firmware, default credentials, and insecure provisioning. Additionally, operational constraints and challenges such as skill shortages, incomplete security posture across environments, and inconsistent security governance create gaps and overlaps in an organization's defenses, providing opportunities for coordinated multi-step attacks.

The research findings suggest an acute need for a more unified, end-to-end approach to VoIP security, where traditional layered and siloed strategies are no longer enough in an era of cloud-first, software-driven, mobile, IoT, and cross-border, geographically-distributed digital workforces. A more integrated approach to VoIP security is necessary, where controls and countermeasures for protocol hardening, network segmentation, endpoint governance, visibility, and continuous monitoring, and administrative controls are designed to operate in concert as part of a system of layered and mutually-supporting defenses.

The Unified VoIP Security Framework (UVSF) presented here was developed in response to this need and gap. The multi-pillar, cross-layered framework seeks to address the primary sources of vulnerability in modern VoIP environments by articulating a holistic set of design principles and concrete controls that can be used to increase VoIP security resilience at each layer of the VoIP communications stack. By emphasizing solutions and countermeasures in each of these key areas – including mandatory encryption, SIP/RTP normalization, segmentation, and secure tunneling

for the network layer and VoIP-aware monitoring and continuous visibility solutions, along with strong IAM, endpoint governance, and proactive security governance – the UVSF provides a guide for organizations to retool and adapt their approaches to VoIP security.

The research also adds to VoIP security literature by providing a more holistic and contextual analysis of VoIP vulnerabilities. This perspective combines the practical and technical dimensions of VoIP deployment and support with academic analysis to help clarify not just the risks, but also why and how these vulnerabilities manifest. In this way, the study also provides a more nuanced look at how VoIP security may be strengthened not just through advanced technical controls but through the rigorous coordination of people, processes, and technology.

In this way, there is opportunity for future work in this area. This may include quantitative performance and validation of the UVSF, work on AI-augmented predictive security models for VoIP environments, or further research on Zero Trust architectures for unified communications. As VoIP continues to expand into cloud-native, virtualized, software-driven, and mobile contexts, there will be a need for future research and analysis on the next wave of vulnerabilities and countermeasures.

Nonetheless, the time for piecemeal, loosely-integrated approaches to VoIP security has passed. The study shows that holistic and unified approaches are needed. The multi-layered and cross-cutting framework proposed in this study helps to give organizations a starting point for developing the integrated, adaptive, and resilient security that modern VoIP networks require.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Ahmadzadegan, M. H., Elmusrati, M., and Mohammadi, H. (2013). Secure communication and VoIP threats in next generation networks. International Journal of Computer and Communication Engineering, 2(5).

[2] Akshay, C., Bhavya, C., and Suman, M. (2014). Analysis of security issues in VoIP. International Journal of Computer Applications, 103(8), 1–6. https://doi.org/10.5120/18092-9148

[3] Al Hasib, A., Azfar, A., and Morshed, M. S. (2010). Towards public key infrastructure–less authentication in Session Initiation Protocol. International Journal of Computer Science Issues, 7(1). ttps://doi.org/10.48550/arXiv.1002.1160

[4] Alsubaei, F., and Abdrabou, A. (2021). Cybersecurity workforce and skill shortages: Implications for real-time communication systems. Journal of Cyber Policy, 6(2), 241–259.

[5] Anwer, A., Shahid, M., and Ni, Q. (2018). The challenges of 5G in a cloud-based network. ComSoc Technology News. https://www.comsoc.org/publications/ctn/challenges-5g-cloud-based-network

[6] Azfar, A., Choo, K.-K. R., and Liu, L. (2016). Android mobile VoIP apps: A survey and examination of their security and privacy. Electronic Commerce Research, 16(1), 73–111.

[7] Baugher, M., et al. (2004). The secure real-time transport protocol (SRTP) (RFC 3711). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc3711

[8] Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27–40. https://doi.org/10.3316/QRJ0902027

[9] Bugeja, G. B., and Fibian, A. C. (2011). Voice over IP security (Chapter: VoIP vulnerabilities, attacks, and countermeasures). Springer.

[10] Carrillo-Mondéjar, J., Martínez, J. L., and Suárez-Tangil, G. (2022). On how VoIP attacks foster the malicious call ecosystem. Computers and Security, 117, 102713.

[11] Dantu, R., Fahmy, S., Schulzrinne, H., and Cangussu, J. W. (2009). Issues and challenges in securing VoIP. Computers and Security, 28(8), 743–753.

[12] Dassouki, K., Safa, H., Mohammed, N., and Abbas, H. (2017). Protecting from cloud-based SIP flooding attacks by leveraging temporal and structural fingerprints. Computers and Security, 104, 65–75. https://doi.org/10.1016/j.cose.2017.08.003

[13] Dharmin, S., and Parag, R. (2020). A comprehensive study of VoIP security. In 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN). https://doi.org/10.1109/ICACCCN51052.2020.9362943

[14] Dimitris, G., Kambourakis, G., Dagiuklas, T., and Lambri, C. (2005). SIP security mechanisms: A state-of-the-art rview. IEEE Security and Privacy.

[15] Ezzah, F., Irshad, A., and Rania, N. (2024). A comprehensive survey on security threats and challenges in cloud computing models (SaaS, PaaS and IaaS). Journal of Computing and Biomedical Informatics, 7(1).

[16] Flick, U. (2018). An introduction to qualitative research (6th ed.). SAGE Publications.

[17] Francis, N., and Nweso, N. (2014). VoIP security: Threats and countermeasures. Researchjournali's Journal of Computer Science, 1(16).

[18] Fukuyama, N., and Fujimoto, S. (2016). Firewall-friendly VoIP secure gateway and VoIP security issues. Fujitsu Scientific and Technical Journal, 39(2), 182–188.

[19] Galiotos, P., Anagnostopoulos, C., Dagiuklas, T., and Kotsopoulos, S. (2016). Non-conforming behavior detection for VoIP-based network systems. IEEE International Conference on Communications.

[20] Jabra. (2020). How to drive UC user adoption in an organization. https://www.jabra.com/blog/how-to-drive-unified-communications-user-adoption-in-an-organization/

[21] Joachim, K., Dirk, P., and Manuela, R. (2017). Digital transformation and the challenges for organizational communications. In Out-thinking Organizational Communications (pp. 1–6). https://doi.org/10.1007/978-3-319-41845-2_1

[22] Karapantazis, S., and Pavlidou, F.-N. (2009). VoIP: A comprehensive survey on a promising technology. Computer Networks, 53(12), 2050–2090.

[23] Keromytis, A. D. (2010). A comprehensive survey of voice over IP security research. IEEE Communications Surveys and Tutorials.

[24] Kuhn, D. R., Walsh, T. J., and Fries, S. G. (2005). Security considerations for Voice over IP systems (NIST SP 800-58). NIST.

[25] Lee, I. (2008). A novel design of a VoIP firewall proxy to mitigate SIP-based flooding attacks. International Journal of Internet Protocol Technology, 1(2/3), 179–186.

[26] Macnish, K., and van der Ham, J. (2020). Ethics in cybersecurity research and practice. Technology in Society, 63, 10182. https://doi.org/10.1016/j.techsoc.2020.101382

[27] Mohd Ramly, A., Ng, Z. W., Khamayseh, Y., Kwan, C. S. C., Amphawan, A., and Neo, T.-K. (2024). Review and enhancement of VoIP security: Identifying vulnerabilities and proposing integrated solutions. Journal of Telecommunications and the Digital Economy, 12(4), 109–136. https://doi.org/10.18080/jtde.v12n4.1022

[28] Nazih, W., Elkilani, W. S., Dhahri, H., and Abdelkader, T. (2020). Survey of countering DoS/DDoS attacks on SIP-based VoIP networks. Electronics, 9(11), 1827. https://doi.org/10.3390/electronics9111827

[29] NIST. (2005). Security considerations for Voice over IP systems (SP 800-58, Rev. 1).

[30] Nowell, L. S., Norris, J., White, D. E., and Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. International Journal of Qualitative Methods, 16, 1–13. https://doi.org/10.1177/1609406917733847.

[31] Nuño, P., Suárez, C., Suárez, E., and Gonzalez Bulnes, F. (2020). A diagnosis and hardening platform for an Asterisk VoIP PBX configuration vulnerability assessment. Journal of Information Security and Applications, 55, 102–115.

[32] Paramasivam, I., and Qubeb, S. M. P. (2019). Research on security architecture for cloud-based VoIP using Hadoop clusters. International Journal of Engineering and Advanced Technology, 8(6), 3708–3714.

[33] Phithakkitnukoon, S., and Weber, I. (2008). VoIP security: Attacks and solutions. Journal of Information Security and Applications, 13(5), 387–395.

[34] Saenger, J., Arndt, M., and Schürmann, T. (2020). VoIP network covert channels to enhance privacy and data exfiltration. Computer Networks, 169, 107–120.

[35] Seokung, Y., Park, H., and Hyeong, S. (2013). Security issues on mobile VoIP. Journal of Computational and Theoretical Nanoscience, 19(8), 2149–2152. https://doi.org/10.1166/asl.2013.4953

[36] Sven, E., Dimitris, G., and Thomas, M. (2010). Survey of network security systems to counter SIP-based denial-of-service attacks. Computers and Security, 29(2), 225–243.

[37] https://doi.org/10.1016/j.cose.2009.09.004

[38] Tuleun, W. (2024). Design of an Asterisk-based VoIP system and the implementation of security solution. World Journal of Advanced Research and Reviews, 23(1), 875–906. https://doi.org/10.30574/wjarr.2024.23.1.2048

[39] Unified Communication and Collaboration. (2020s). A key driver of digital transformation. Fujifilm Business Innovation.

[40] Valerie, J. M., Sohrab, M., and Patti, F. (2010). VoIP for telerehabilitation: A risk analysis for privacy, security, and HIPAA compliance. International Journal of Telerehabilitation, 2(2), 3–14. https://doi.org/10.5195/ijt.2010.6056

[41] Vuong, S. T., and Bai, Y. (2004). A survey of VoIP intrusions and intrusion detection systems. In Proceedings of ICACT 2004.

[42] Wu, Y.-S., Apte, V., and Bagchi, S. (2009). Intrusion detection in Voice-over-IP environments. International Journal of Information Security.

[43] Younes, O., and Albalawi, U. (2022). Securing Session Initiation Protocol. Sensors, 22(23), 9103. https://doi.org/10.3390/s22239103