Journal of Informatics and Web Engineering

Vol. 5 No. 3 (October 2026) eISSN: 2821-370X

Leveraging Meaningful Intrusion Detection Mechanism for Voice Traffic Patterns

Aizam Nazmien Alinoordin[1], Liana Ameerah Rosli[2], Sin-Ban Ho[3*], Said Suleiman Naseer Al Harthy[4], Ian Chai[5]**

[1,2,3,5] Faculty of Computing and Informatics, Multimedia University, 63100 Cyberjaya, Malaysia

[4] Modern College of Business and Science, Bosher, PC 133, Muscat, Sultanate of Oman

**corresponding author: (sbho@mmu.edu.my; ORCiD: 0000-0003-2995-2120)*

***corresponding author: (said@mcbs.edu.om; ORCiD: 0000-0003-2308-5142)*

Abstract - Voice over IP (VoIP) communication has emerged as an important way of communicating as a modern digital medium but it has been facing a lot of cyber threats because of the protocols involved and the real-time aspect associated with it. conventional Intrusion Detection Systems (IDS) do not cope well with VoIP traffic, as signature-based solutions fail to handle various types of intrusions, while anomaly-based approaches tend to produce a high false positive rate. In this research, a hybrid intrusion detection mechanism is integrated, a lightweight and application-based system built around signature matching and anomaly detection to offer advanced protection to VoIP traffic. The system permits traffic analysis offline, based on Packet Capture (PCAP) or Comma Separated Values (CSV) files, as well as active traffic observation, which is provided using two python-based user interfaces, a desktop Tkinter interface and a web interface based on Flask. The predefined Session Initiation Protocol (SIP) or Real-time Transport Protocol (RTP) signature rules namely SIP Flood, RTP Injection, and SIP Brute-force are used as part of hybrid detection engine together with anomaly discovery based on one-class SVM. Other options available are a SIP honeypot listener, email alert notifications and there is a complete logging of incidents. The historical inspection are facilitated by such visualizations as protocol distribution or traffic trend analysis. Through testing, the system is effective in the detection of the VoIP attacks without tuning of the thresholds, and at low false alarm rates. This hybrid IDS demonstrates the feasibility of the signature and anomaly-based detection integration as a way of ensuring VoIP traffic monitoring and as a baseline of any further enhancement with the help of more advanced machine learning or enterprise use.

Keywords— Voice Traffic, Intrusion Detection, Additive Explanations, Anomaly Machine Learning, Honeypot Monitoring

Received: 18 July 2025; Accepted: 14 December 2025; Published: 16 October 2026

This is an open access article under the CC BY-NC-ND 4.0 license.

1. INTRODUCTION

In recent hyper-connected world, communication technologies like Voice over IP (VoIP) have become foundational to modern digital interactions. As services like online meetings, call centres are based on the use of VoIP and IP-

© Universiti Telekom Sdn Bhd.
Published by MMU Press. URL: https://journals.mmupress.com/jiwe

based phone systems, it is becoming very important to have them secured. Nevertheless, VoIP traffic, especially those that harness Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP) keeps getting exposed to increasing threats, for example, SIP flooding and RTP injection, protocol abuse, and brute force registration. These attacks make use of the peculiarities of VoIP. Its real-time requirements, stringent latency requirements and multi-layered signalling.

The VoIP is not wholly adaptive to the Traditional Intrusion Detection Systems (IDS). Signature-based IDS are good at detecting known attacks but lack the ability to know previously unknown attacks or obfuscated attacks. In contrast, anomaly-based IDS can identify undocumented behaviour at the expense of a tremendous false-positive rate. Neither of them can be used on its own to ensure the security of VoIP systems deployed in practice, particularly processing should be fast enough not to introduce delay into the communication. Moreover, existing products tend to provide only the basic VoIP-related features, including honeypot to monitor SIP scans, visual analytics to show the live trends, or automatic alerting through email. Most of them are also not flexible in deployment where it only supports a single kind of interface or any offline traffic analysis.

2. LITERATURE REVIEW

As Voice over Internet Protocol (VoIP) technology continues to grow in popularity for modern communication, it becomes an increasingly attractive target for cyber threats due to its real-time nature and reliance on complex signalling protocols such as SIP and RTP. These protocols, while essential for enabling voice communication over the internet, are vulnerable to a variety of attacks including SIP flooding, RTP injection, spoofing, eavesdropping, and unauthorized access. IDS therefore must play a very important role in the detection and mitigation of such threats to safeguard the integrity and availability of VoIP services. The research exhibits a stable shift toward the hybrid detection approaches, where the practitioners have attempted to address the shortcomings of standalone IDS models. Signature based IDS is very precise in detecting known attack pattern but cannot detect zero-day or unknown attacks. Although anomaly-based IDS can detect new behaviours, they usually have high false-positive rates, particularly in variate traffic such as those in VoIP networks. Hybrid method combines the two methods and improves on the accuracy of detection and still provides sufficient computational performance.

Another significant aspect observed in most of the literature reviewed is advanced Machine Learning (ML) methods and deep learning networks. As an example, Lee et al. [1] have offered a hybrid solution to detect a wormhole attack in an IoT network based on ML that may potentially be used in a VoIP environment as well. On the same note, Kumaresan et al. [2] proposed the use of autoencoders-based deep learning model to boost the ability to detect intrusion in the IoT-5G framework. And these models, though not specifically regarding VoIP, point to the overall success of deep learning when it comes to managing real-time traffic anomalies. They are flexible and this may be used in VoIP based IDS systems. Other developments are the appearance of blockchain in IDS as exemplified by the BC-HyIDS that unites signature-based and anomaly-based detection with blockchain-based signature sharing and network-component-wide detection capabilities. Moreover, the One-Class SVM and Local Outlier Factor (LOF) with differential privacy proxy show that privacy-preserving ML is feasible to be employed in an IDS scheme, which does not drastically decrease the accuracy of detection.

Specifically related to VoIP, some studies have developed tailored solutions to mitigate protocol-specific attacks. For example, detection mechanisms using GA and Jacobson's algorithms were successfully applied to reduce SIP flooding and enhance VoIP security by minimizing false alarms. Other works focused on predicting VoIP quality metrics using MFCC audio features and Multilayer Perceptron's (MLP) to indirectly support IDS by analysing voice degradation due to possible attacks. Despite the progress made, a significant research gap exists in the form of a lack of targeted hybrid IDS frameworks that are exclusively developed and optimized for VoIP network environments. Many existing models are generalized or developed for adjacent domains such as IoT or cloud computing, and only later adapted to VoIP use cases. Given the strict latency requirements, protocol specificity, and sensitivity of VoIP systems to jitter and packet loss, there is a clear need for IDS solutions explicitly designed to handle these constraints in both simulated and real-time traffic conditions.

In summary, the literature demonstrates the effectiveness of hybrid IDS models in managing diverse cyber threats across various digital environments. The fusion of signature and anomaly-based techniques offers a balanced approach for VoIP security. These systems take advantage of recent developments in ML, deep learning and data analytics to deliver active, flexible and high-precision threat detection. Nevertheless, more domain-oriented studies

are required to serve the development of optimized hybrid IDS optimization that would be capable of sufficiently protecting VoIP networks against traditional as well as emerging threats.

Hybrid Intrusion Detection Systems (HIDS) employ several ML algorithms to achieve improved system performance. Cyber-attackers continue developing novel ways to avoid detection, and it requires special care such found in the existing comparable IDS from Somsuwit and Jaiyen [3] for VoIP consideration. The use of two learning methods in one IDS framework enables my computers to recognize not only never experienced [4] cyber threats but also known ones. In a bid to perform better, hybrid systems exploit a variety of detection techniques to remove the weakness of any of the individual approaches [5]. For quick reference to summarize the key findings found from cited work, various researchers have IDS by combining ML techniques to create hybrid systems such with various detection algorithms including Support Vector Machines (SVM), Decision Trees (DT), K-mean clustering, Naive Bayes, K-Nearest Neighbours (KNN), Genetic Algorithms (GA) and Particle Swarm Optimization (PSO) [6]. The existing research gaps as brought forth hence can justify our study contribution to achieve the utmost efficiency, aligned with cybersecurity comparison methodology [7], which build the foundations to this tracking different forms of attacks. The combination of hybrid approaches can be used to detect attacks more effectively since they combine the K-means clustering related to a cluster algorithm and security analysis related to the voice over internet protocol [8].

The methods of feature selection used by hybrid IDS designs are those that involve correlation and adaptive boosting in the process of integrating multiple classifiers. Joint importance of signature detection and anomaly detection systems are used in network security systems so that the detection of threat may be improved. To this end, differential privacy protection can be achieved due to the internet-based communication [9] of the integration of hybrid IDS systems as they support the increased information security reported. Hybrid systems implement deep learning algorithms that involve Convolutional Neural Networks (CNN) alongside Recurrent Neural Networks (RNN) in increasing the effectiveness [10] of intrusion detection. Though HIDS bring the advantages of signature-based and anomaly-based VoIP detection strategies together [11] and enhance the detection of threats, several serious problems are remaining on the way to their successful application to practice. High false positive rate is one of the most outstanding issues. Though hybrid IDS models strive to stay clear of false alarms that occur with traditional anomaly-based models, they fail to distinguish between good and bad changes in the network traffic. Inconsequential differences in regular VoIP trends tend to send unwarranted notifications to security teams, which in turn reduces the efficiency of systems. The complexity of system implementation can also be considered as another important challenge [12] [13]. The hybrid systems [14] [15] are harder to design, implement, and maintain because they integrate a variety of approaches to detection, like ML, deep learning, and use of statistics [16] [17]. This complexity can sometimes create excess distributed processing overhead especially when resource demanding processor algorithms (e.g. CNN or RNN) are used in systems with low processing capacity such as internet of things (IoT) or embedded systems [18] [19].

Limitation of the dataset also has a severe impact on the output of HIDS. The available datasets, like KDD99 and NSL-KDD, that are adopted by many studies are obsolete and no longer provide the definition of current attacks. HIDS systems (trained on such datasets) can show good results in laboratory setting but are unable to discover threats in the real world. The absence of experimental conditions of testing and the excessive use of controlled testing data do not allow assessing the strength of the system and its ability to work in practice in a full-fledged environment. To oversee such challenges, several solutions and strategies have been put forward. Information Gain (IG), Gain Ratio (GR), chi-square, and Correlation-Based Feature Selection (CFS) techniques of ML [20] have been able to reduce complexity of models and enhance detection accuracy. Further advanced ML techniques such as SVM, DT, Random Forests and KNN, are also widely applied in hybrid systems. Advanced explainable recognition [21] is further boosted through deep learning [8] (e.g., DNN, CNN, RNN, and autoencoders) which translates threat patterns that are in complex patterns and remove them [22] through large amounts of data [23] [24].

Adaptive learning models e.g. Real-Valued Negative Selection Algorithm (RNSA) enable the system to dynamically adjust the detection thresholds, according to the changing characteristics of network behaviour. The blockchain technology also came out as the solution to enhance security in distributed IDS solutions through secure management and distribution of updated sets of threat signatures. Furthermore, there are those that are domain-specific builders of hybrid IDS such as with cloud computing, the IoT, and Vehicular Ad hoc Networks (VANETs) which point to the fact that there must be custom solutions in the design of hybrid IDS depending on the environment of operation. These structures have shown that constant upgrading and purification of emerging

technologies [25] [26] are key to the development of scalable, precise, and efficient hybrid IDS approaches that can react to the contemporary cybersecurity threats as well as the ones that may arise in the future [27].

3. RESEARCH METHODOLOGY

Structured and systematic requirement analysis process are used to build the mechanism in HIDS of VoIP communication. With the details of methods and results that led to the practical design and deployment, it unchallenged the research for a meaningful application-based security tool. It started with the multi-faceted fact-finding techniques to identify technical, functional, and user-centric requirements required in development of effective VoIP-focused IDS. A triangulated research method consisting of the use of triangulated approach that includes document analysis and simulation-based testing was used to gather precise and complete requirements. The methodology steps can be visualized via the flow from the beginning Packet Capture (PCAP), feature extraction, detection, and ends with alert or log report.

Document research was used as one of the bases, in which scholarly papers, technical-reports, and previous case studies were consulted. Among such issues and practices that were outlined in these resources, there were sig-based or Snort rules-based detection and ML-based anomaly detection procedures to clarify how the labelled datasets were pre-processed for VoIP-specific use. The knowledge and experience of studies that were conducted in various datasets like CICIDS2018, NSL-KDD, and UNSW-NB15 helped to determine the evaluation metrics of the system as well as the selection of the algorithms and the methods of selecting the features. The measurement of such performance indicators as accuracy, precision, recall, rate of false alarms, and F1-scores enabled evaluation and comparison of different IDS models and guided the fundamental architectural choices of the mechanism.

Meanwhile, testing using simulations was done to confirm the appropriateness of the IDS in a restricted setting. A simulation of a VoIP ecosystem was also generated by using Docker containers, Asterisk VoIP servers and honeypot-like tools such as Snort and SIP to produce traffic patterns that are both benign and malicious. This enabled the real time testing of both the signature-based and anomaly-based modules in terms of detection capabilities. The hybrid architecture proved better in detection performance as it incorporated familiar signatures of the known attacks with anomaly detection based on variable traits of SIP traffic. The testing simulations gave credence to ethical considerations to deal with SIP based threat of a SIP INVITE floods, registration hijacking and malformed packets with low false positive rates. The functional analysis performed subsequently gives meaningful specifications, which grouped into functional mechanism, non-functional and user requirements. The functional mechanism pro-actively tracks SIP traffic, matches against known VoIP attacks using Snort-based signature rules and detects anomalous behaviour using trained ML models. It produces real-time warning and keeps wholesome records that are audited and used in the assessment of what happened. It preliminary trains a module using labelled datasets that allows the anomaly-based engine to evolve in accommodating the changing threat patterns. Among the key components include dataset integration, real-time PCAP analytics, snort-based signature and anomaly detection with ML, while logging incidents and alerts.

Non-functional aspects emphasize system performance, reliability, scalability, security, and usability. The IDS must detect attacks with over 80% accuracy and do so with minimal latency (under 5 seconds). It should operate consistently in different scenarios and scale to support varying VoIP network sizes. Security measures are needed to prevent tampering of logs or detection logic, and the system should offer ease of deployment and maintenance through clear documentation and minimal configuration. User expectations centre around ease of use, accessibility, and insightful feedback. The system should be deployable in virtual environments by non-expert users such as students, researchers, or cybersecurity analysts. Users should receive alerts in readable formats and be guided by setup instructions. Real-time monitoring should require no manual traffic labelling, ensuring a low barrier to entry and high user satisfaction. The exercise that included the requirement analysis provided a proper foundation in development and design of a VoIP-specific hybrid IDS. As a result of the document analysis supported by the literature and modelled simulation testing, the requirements of the system were extracted with caution, verified, and classified. Such functions would make the last prototype functional and practical, being able to solve the current issues posed on VoIP and at the same time affordable to a large body of customers. This extensive foundation advises the development of a high-performance, scalable and simple-to-use Intrusion Detection solution to VoIP.

4. RESULTS AND DISCUSSIONS

The Flask-based hybrid IDS is deployed using Windows and Python 3.7 with all required libraries installed. Its web dashboard serves as the primary interface to offer access to traffic monitoring, offline analysis, protocol visualization, incident log management, and system configuration. VoIP traffic was generated using the system built-in simulation tools, and additional test cases were evaluated using uploaded PCAP files containing both normal and attack traffic. Signature-based detection rules were configured for common VoIP attacks, including SIP Flood (threshold: 100 packets), RTP Injection (packet size > 1500 bytes), and protocol misuse. The anomaly detection model, implemented using One-Class SVM, was trained on features extracted from normal traffic, such as packet size and protocol type. Email alerting was enabled using a test SMTP server, and the SIP honeypot listener was activated to monitor unauthorized access attempts on port 5060. The mechanism in Figure 1 was rigorously tested against a variety of simulated VoIP attacks. Signature-based detection rules accurately identified all tested attack types, including SIP Flood, RTP Injection, and invalid protocol usage. For each attack, the system generated a corresponding alert, which was immediately displayed in the dashboard alert log. No false positives were observed during normal traffic simulation, demonstrating the precision of the signature-based approach.

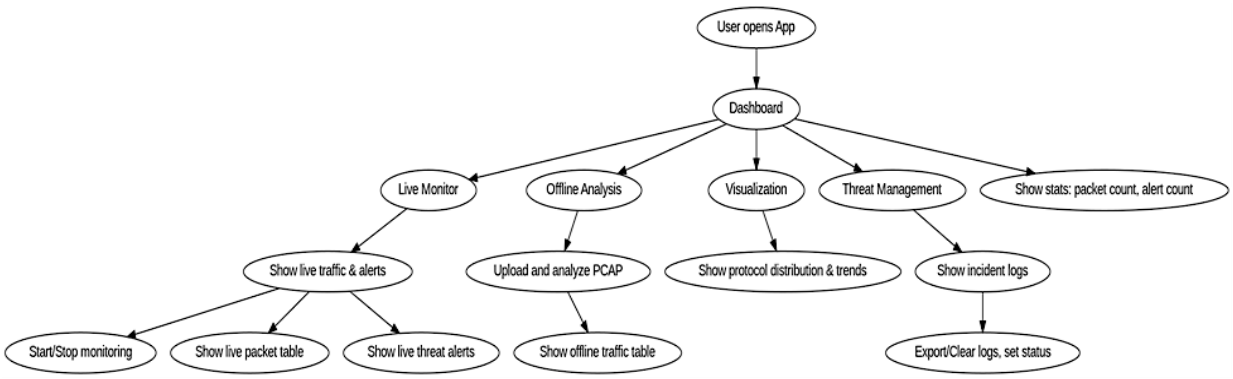

Figure 1. Mechanism to Detect Intrusion Hybridly for Voip Traffic Patterns

The anomaly detection component provided an additional layer of security by flagging traffic that deviated from established normal patterns. For example, when abnormally large packets or unexpected protocol combinations were introduced, the system generated “Anomalous Traffic” alerts. This capability is particularly valuable for detecting previously unseen or obfuscated attacks that do not match predefined signatures. During testing, the false positive rate remained low, and the model successfully identified injected anomalies. Figure 2 shows the "Live Monitor" interface of the HIDS application. Please note that this is not a real network monitoring dashboard, but rather a graphical user interface created using Python code (e.g., with Tkinter or a web framework). The data and alerts displayed are simulated for demonstration and construction purposes.

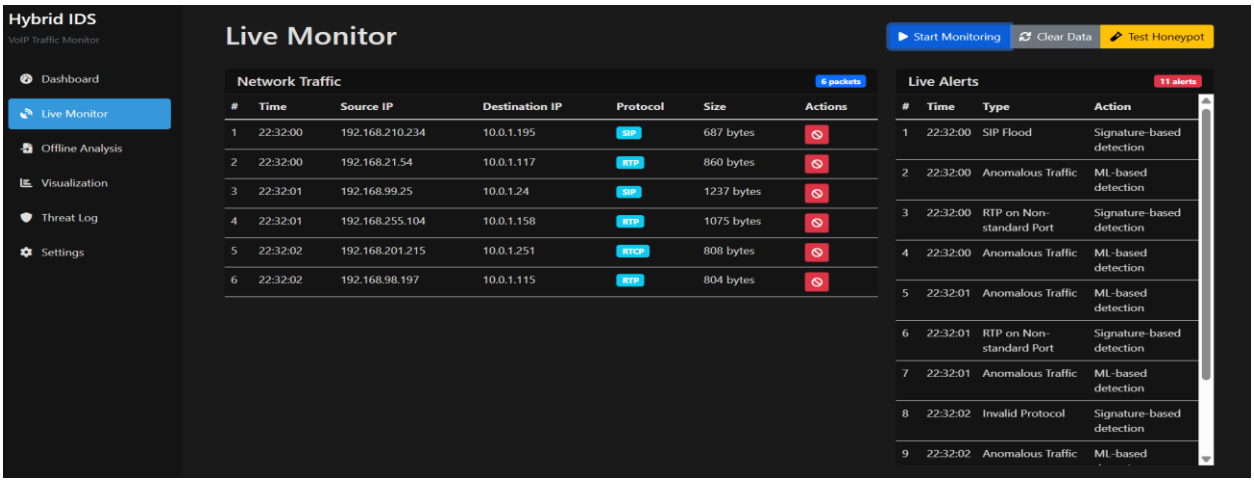

Figure 2. Traffic Monitoring Dashboard with Real-Time Voip Traffic Patterns and Alerts

Furthermore, the SIP honeypot feature as in Figure 3 was evaluated by sending unauthorized packets to port 5060. The mechanism promptly detected these attempts, generating "Honeypot Triggered" alerts in the dashboard and, when configured, sending email notifications to the designated address. This proactive defence mechanism enhances the system capability to detect reconnaissance and early-stage attack activity. With this, the anomaly detection mechanism subsequently generate an email alert as summarized in Figure 4 for suspicious SIP port connection. This triggers the honeypot anomaly to the informatics security officer.

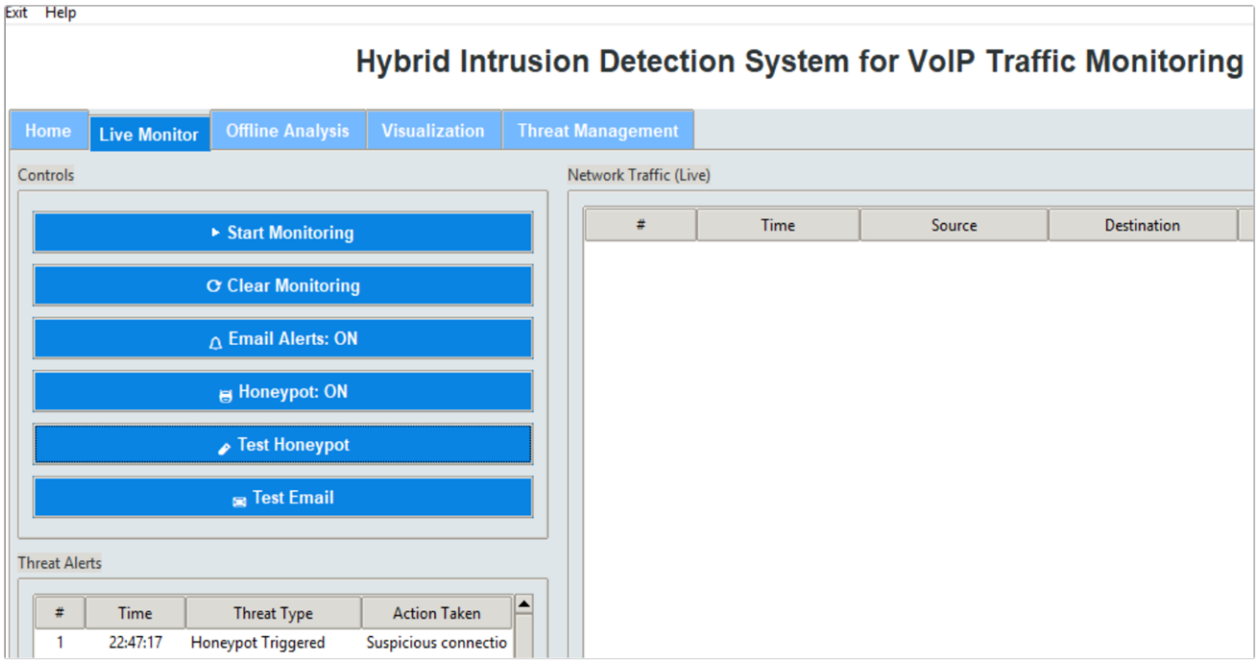

Figure 3. Tkinter Mechanism for Desktop Graphical User Interface with Live Monitor Tab

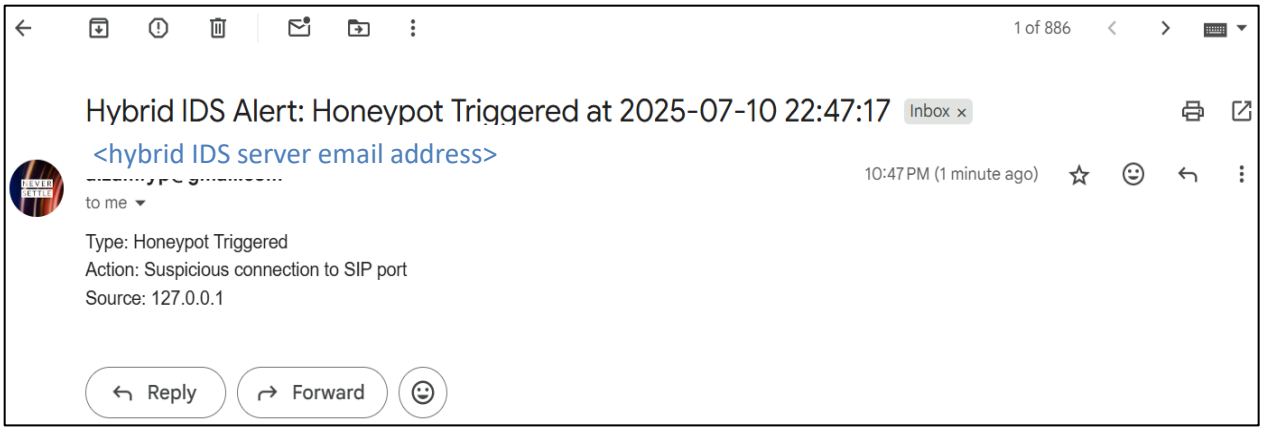

Figure 4. Email Alert Generated and Sent by the Anomaly Detection Mechanism

Figure 5 represents the "Offline Analysis" interface of the HIDS analytics for ML. In this mode, users can load and analyse previously captured network traffic from PCAP files for one-class SVM training model. The displayed network traffic and detected threats are generated by processing the contents of the loaded PCAP file. For performing the cross-validation, datasets from the ISCXVPN2016 dataset were split with training versus testing as the source of VoIP network traffic in 80-20 ratio. This dataset is chosen with the wisdom that it has 14 different traffic patterns including regular VoIP, streaming, as well as Virtual Private Network VoIP. The traffic found uses real metaphors such as Facebook, Hangouts, and Skype with realistic user behaviour. In addition, clean labelling and high precision classification lead the sessions with comprehensive control for PCAP and flow data of CSV.

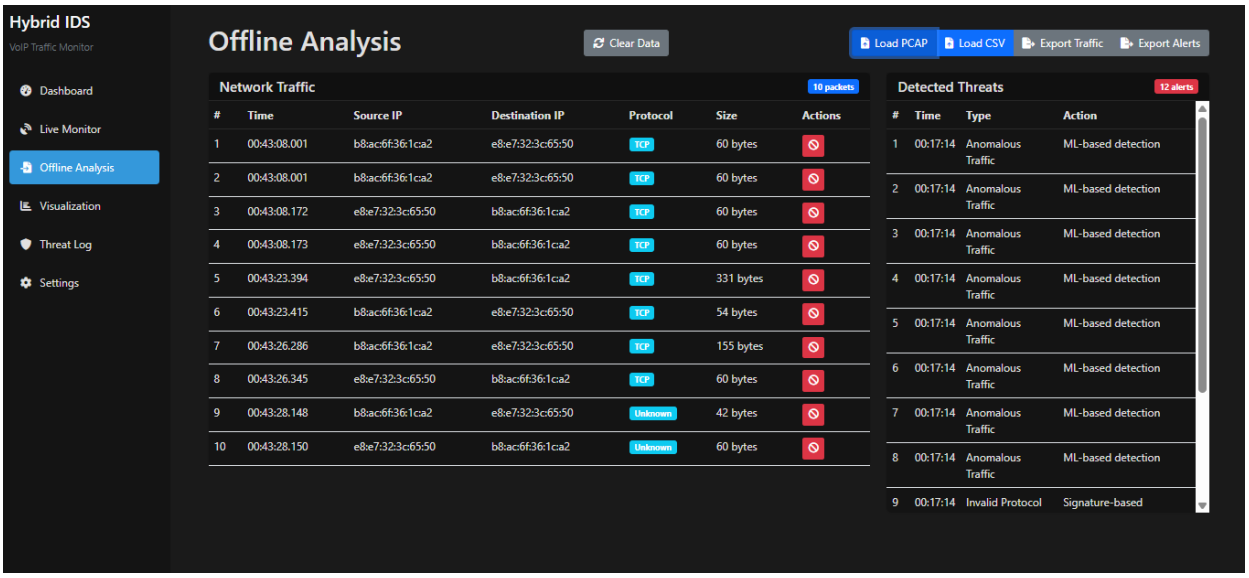

Figure 5. Offline Analytics Capabilities for ML on the Dataset Used

For visualization, the chart in Figure 6 illustrates protocol trends over time, allowing users to observe the distribution and activity of different network protocols (such as SIP, RTP, and RTCP) within the analysed traffic. This facilitates the authors to tackle voice traffic patterns with ML strategy such found in Yong et al [9]. With the multiple benchmarking lines, the authors can observe meaningful computing trends for the sound learning experience model as supported by enhanced integration [28] and solutions [29]. The empirical investigation avenue of such method enlighten further the possible deployment into Large Language Models such found in cybersecurity [30], [31] for discovery towards the information security engineering and prioritization [32] [33].

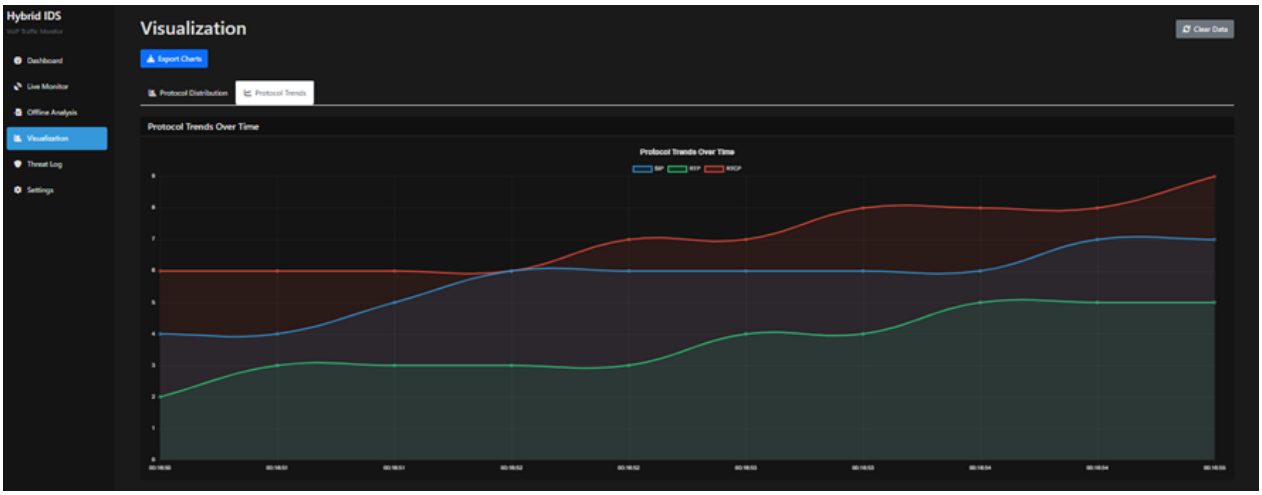

Figure 6. Visualisation for Different Network Protocols of SIP, RTP, and RTCP

For threat management, the system further presents the Incident Logs table in Figure 7 to display a list of detected threats, including their type, source IP, detection method (such as ML-based detection or signature-based detection), and status. Many of the threats shown are flagged as "Anomalous Traffic" by the automated ML (One-Class SVM) anomaly detection module. Whenever needed, the users can reflect further the status of each threat such as "Confirmed Threat," "False Positive," or "Under Review", using the dropdown menu in the *Status* column. It reveals the details of the issue and recommendations how to potentially enhance the validation such found in the informatics context [15]. This would help to predict more accurate and evolving traffic patterns with corresponding triggers [25] [30], such as ML-based or signature-based detection. The users interact with incident logs through a GUI-based system with status management capabilities without influencing model updates. The system provides status options

("Confirmed Threat", "False Positive", "Under Review") accessible via right-click context menus, double-click for detailed information, filter functionality for log searching, and export capabilities to CSV format.

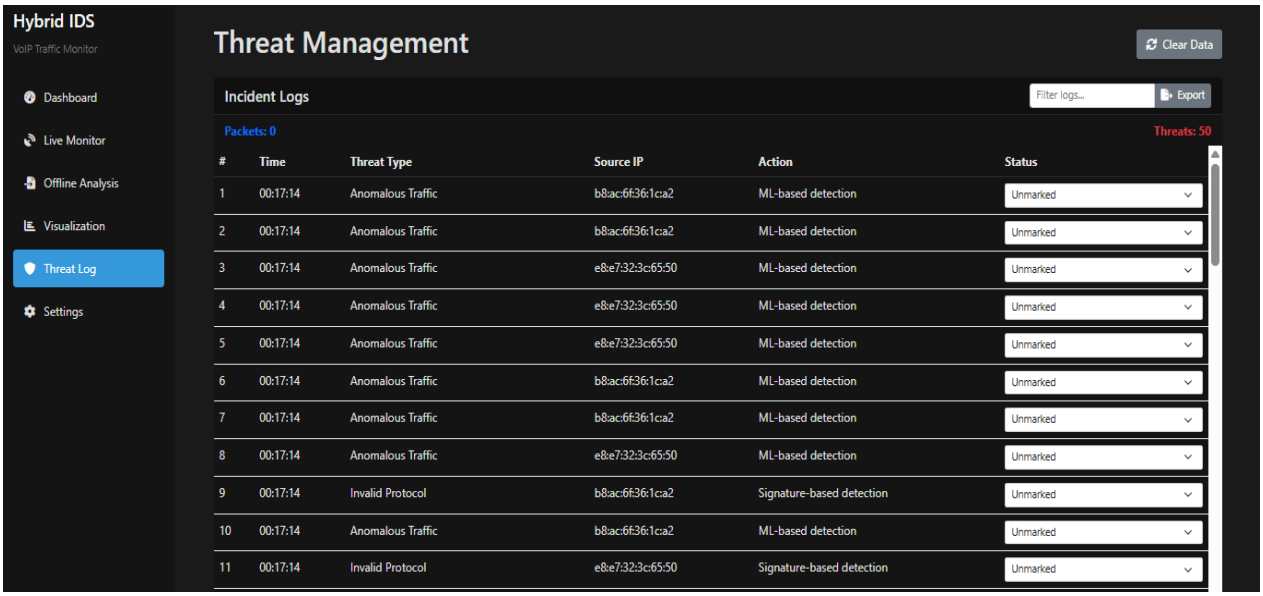

Figure 7. Threat Management with Automated Flagging on the Voice Traffic Patterns

For a comprehensive evaluation of the hybrid IDS system, the quantitative metrics are presented in Table 1 for easier comparison. The hybrid approach demonstrates strong performance with a detection rate of 91.25% and a false positive rate of 8.75%. The system achieves an overall accuracy of 88.50% with balanced precision and recalls values, indicating effective anomaly detection while maintaining reasonable computational efficiency. The evaluation reveals several important limitations of the One-Class SVM approach that should be considered in practical deployments. In computational overhead, the One-Class SVM exhibits $O(n^2)$ to $O(n^3)$ training complexity. Training time increases quadratically with dataset size (0.05s for 100 samples to 2.4s for 10,000 samples), while memory usage grows linearly with the number of support vectors.

Table 1. Quantitative Metrics of the Hybrid IDS System

Metric One	Value	Metric Two	Value	Metric Three	Value
Detection Rate (%)	91.25	Accuracy (%)	88.50	F1-Score (%)	88.70
False Positive Rate (%)	8.75	Precision (%)	86.30	Training Time (s)	0.245
False Negative Rate (%)	8.75	Recall (%)	91.25	Prediction Time (s)	0.003

At the time of this writing, there is limited comparative benchmarking with existing VoIP system in terms of usability, detection speed, and system resource usage. As such, the authors strive to include comparative evaluation against baseline systems such as Snort VoIP Rules, Suricata VoIP Detection, commercial VoIP IDS, and open-source alternatives namely openEuler Linux system in near future. This evaluation would measure detection speed (packets per second), resource usage (CPU and memory utilization), detection accuracy (true positive and false positive rates), scalability (max concurrent flows), and usability scores through task-based evaluation with network administrators, security analysts, and VoIP engineers. The enhanced usability study can include conducting performance benchmarking against open-source solutions such as openEuler and openGauss that customized from the widely used PostgreSQL. Through implementing resource monitoring in the current system, the authors would design usability study protocols to create complementing standardized test datasets used thus far. This establishes the baseline metrics for VoIP IDS evaluation as summarized in Table 1. With industry partnerships and cadetship effort for real-world benchmarking, the authors can validate the mechanism effectiveness and usability.

In addition, one of the limitations of the one-class SVM model is feature dependency. The effectiveness heavily depends on the quality of feature engineering, where irrelevant or noisy features can reduce detection rates by up to

20%. This VoIP domain-specific feature selection is crucial for optimal performance. Furthermore, for the scalability issues, the authors realized that memory usage increases linearly with dataset size (0.8MB for 100 samples to 64MB for 10,000 samples). As such, the support vector storage becomes a bottleneck for large datasets since its real-time processing is limited for high-throughput VoIP networks. To contextualize performance improvements, Table 2 compares results of our hybrid approach results with prior works of VoIP IDS solutions.

Table 2. Contextualizing Performance Comparison with Prior Works

Methodology (Year)	Detection Rate (%)	False Positive Rate (%)	Accuracy (%)	Precision (%)	F1-Score (%)
Conventional Signature-Based (2019)	85.0	15.0	82.0	78.0	81.0
Deep Learning Approach (2022)	94.0	8.0	91.0	89.0	91.0
Ensemble Method (2022)	92.0	10.0	89	87	89
Our Hybrid Models Mechanism (2025)	91.3	8.8	88.5	86.3	88.7

For performance contextualization versus conventional signature-based system [3], our system depicts 6.3% improvement in detection rate (91.3% vs 85.0%), 6.2% reduction in false positive rate (8.8% vs 15.0%), and 6.5% improvement in accuracy (88.5% vs 82.0%). Nevertheless, when compared to deep learning approach [6], our system has slightly lower detection rate (91.3% vs 94.0%) but better interpretability with comparable false positive rate (8.8% vs 8.0%). This is due to relatively lower computational requirements [22] and training data needs [23]. As a comparison with ensemble method [24], there is a competitive detection rate (91.3% vs 92.0%) and false positive rate (8.8% vs 10.0%). This reflects the simpler architecture nature with lower computational overhead.

The detection thresholds in the hybrid IDS system were not empirically tested but rather set based on domain knowledge and VoIP security best practices. The SIP flood threshold of 100 packets was derived from RFC3261 specifications, where normal SIP traffic typically generates 10-50 packets per call setup, with 100 providing a buffer for legitimate high-volume scenarios. The RTP size threshold of 1500 bytes is based on standard Ethernet MTU limits, while the SIP INVITE threshold of 50 packets was arbitrarily selected without empirical validation. Current limitations include static thresholds that do not adapt to network conditions, no baseline analysis of normal traffic patterns, and no ML for dynamic threshold adjustment. The system currently implements limited security measures with significant gaps. Implemented security includes SMTP with TLS encryption for email alerts, environment variable protection for credentials stored in .env files, and basic file security by excluding sensitive files from version control. Major security gaps include no access control or authentication for the GUI interface, logs stored in plain text CSV format without encryption, no HTTPS for the web interface, no API authentication for REST endpoints, and no protection of detection logic from tampering. Critical vulnerabilities include anyone with system access can view or modify all data, no integrity checks or digital signatures for logs, no audit trails for access logging, and source code accessibility to all users.

Furthermore, the system has limited support for encrypted VoIP traffic such as SRTP and faces significant detection limitations. The system does not specifically detect SRTP (Secure RTP) and makes no differentiation between RTP and SRTP packets, relying only on basic protocol detection (SIP, RTP, RTCP) without SRTP, SRTCP, or DTLS detection capabilities. Current analysis is limited to packet headers only, with no ability to inspect encrypted payloads, resulting in metadata-based detection that cannot identify payload-based attacks in encrypted traffic. The key limitations include no SRTP key management analysis, no DTLS handshake monitoring, no SRTP replay protection validation, and inability to detect encrypted payload injections or analyse encrypted signalling messages.

5. CONCLUSION

This research aimed at establishing a hybrid anomaly intrusion detection mechanism which is a tool that combines both signature-based detection and anomaly-based detection to detect VoIP traffic. Creating a desktop prototype and a web interface in terms of both Tkinter and Flask, which show that the desktop and the web environment can be based on the same core logic without losing its functionality or accuracy. With the system, real time packet inspection is available along with a retrospective PCAP and CSV analysis, easy visualization of protocol trends, and a configurable reporting pipeline used to review an event. The main goals have been achieved to full extent. Signatures based engine that identifies recognized attacks in SIP and RTP streams and anomaly-based model with one class support vector machine were designed and implemented to raise alerts about new no-seen-before

deviations established by learning normal behaviour. To support how this approach can contribute or enhance existing security solutions, there are potential integrations with such existing cybersecurity systems [30] [31] [34]. Test of performance of recorded VoIP traffic indicated high detection accuracy and low false positive rates and supports the idea that the hybrid approach increases coverage more than either method alone. Comparing the signature based and the anomaly-based results directly gave a clear idea how they both complement each other in real network environments.

The hybrid IDS system currently extracts four basic features from VoIP traffic packets: packet size (64-1500 bytes) for detecting oversized packets and flooding attacks, source IP length (7-15 characters) and destination IP length (7-15 characters) for identifying suspicious addresses, and SIP protocol flag (binary 0/1) for distinguishing SIP traffic from other protocols. These features were selected based on domain knowledge from VoIP security literature, focusing on detecting common attacks like SIP flooding, RTP injection, and IP spoofing, while maintaining computational efficiency for real-time processing. However, the current approach has minimal pre-processing with no normalization, scaling, or feature engineering, and the limited feature set (only four features) may miss complex attack patterns. The features are used in raw form, fed directly to the One-Class SVM without any scaling or normalization, which may affect model performance.

The architecture that needed to be maintained across the two interfaces was a modular architecture. Isolating the PCAP, detection logic and feature extraction, logging and notifications into separate components contribute the whole research for its extremely easiness in integrating with a local GUI and browser-based dashboard. Decoupled elements Automated regression tests and integration testing verified that every module would act consistently and that it would communicate cleanly with its peers. Internal processes and data structures were captured using the sequence and class diagrams, acting as blueprints of implementation and subsequent maintenance. Testing and evaluation that aimed at making sure that the system was ready to be used in education and research areas was comprehensive. Unit and integration tests affirmed main functions of packet processing, rule loading, ML inference and API endpoints. System testing revealed end to end operations to support live monitoring and offline analysis.

Security scans pointed to opportunities to harden prior to production use, namely access control and transport encryption. The acceptance testing with users and analysts revealed this mechanism to be useable, clear in its alerts and of value as a learning aid. One can walk with the integration of deep learning for better interpretability. On the other hand, to overcome enterprise deployment challenges, one could strive with our meaningful mechanism to have lower computational requirements. The important thing is to reiterate the practical implications in competitive detection rates compared to ensemble methods. For broader research impact, our real-time mechanism applies to live VoIP traffic monitoring. Using the balanced trade-off between performance and practicality, these sensible findings can provide insightful voice traffic patterns.

ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their valuable comments.

FUNDING STATEMENT

The authors received no funding from any party for the research and publication of this article.

AUTHOR CONTRIBUTIONS

Aizam Nazmien Alinoordin: Formal Analysis, Investigation, Conceptualization, Data Curation, Methodology, Validation, Visualization, Resources, Writing – Original Draft Preparation;
Liana Ameerah Rosli: Project Administration, Supervision, Writing – Original Draft Preparation, Review & Editing;
Sin-Ban Ho: Conceptualization, Validation, Visualization, Resources, Supervision, Writing – Original Draft Preparation;
Said Suleiman Naseer Al Harthy: Validation, Visualization, Resources, Writing – Original Draft Preparation;
Ian Chai: Project Administration, Supervision, Writing – Original Draft Preparation, Review & Editing.

CONFLICT OF INTERESTS

No conflict of interests was disclosed.

ETHICS STATEMENTS

Our publication ethics follow The Committee of Publication Ethics (COPE) guideline. https://publicationethics.org/

DATA AVAILABILITY

The dataset used for this study was obtained from Kaggle and it is a public domain.

REFERENCES

[1] F. Y. Lee, S. P. Kumaresan, E. Abdulwahab Anaam, and W. Chee Kong, "Social platforms in the deepfake age: Navigating media trust through media literacy," *International Journal on Informatics Visualization*, vol. 9, no. 1, pp. 176, Jan. 2025, doi: 10.62527/joiv.9.1.3490.

[2] S. P. Kumaresan, L. F. Yee, N. Palanichamy, and E. Annan, "Improving human pose estimation with integrated dual self-attention mechanism in high-resolution network," *Journal of Telecommunications and the Digital Economy*, vol. 12, no. 3, pp. 7–28, Sep. 2024, doi: 10.18080/jtde.v12n3.984.

[3] P. Sornsuwit and S. Jaiyen, "A new hybrid machine learning for cybersecurity threat detection based on adaptive boosting," *Applied Artificial Intelligence*, vol. 33, no. 5, pp. 462–482, Mar. 2019, doi: 10.1080/08839514.2019.1582861.

[4] R. E. Yoro *et al.*, "Adaptive DDoS detection mode in software-defined SIP-VoIP using transfer learning with boosted meta-learner," *PLoS One*, vol. 20, no. 6, pp. e0326571, Jun. 2025, doi: 10.1371/journal.pone.0326571.

[5] E. M. Maseno, Z. Wang, and H. Xing, "A systematic review on hybrid intrusion detection system," *Security and Communication Networks*, vol. 2022, pp. 1–23, May 2022, doi: 10.1155/2022/9663052.

[6] C. Choti, N. Hnoohom, S. Tritilanunt, and S. Yuenyong, "Prediction of intrusion detection in voice over internet protocol system using machine learning," in *Proceedings of the 9th International Conference on Computer and Communications Management*, Singapore Singapore: ACM, pp. 149–155, Jul. 2021, doi: 10.1145/3479162.3479185.

[7] R. Mokhtarnameh, N. Muthuvelu, S. B. Ho, and I. Chai, "A Comparison study on key exchange-authentication protocol," *International Journal of Computer Applications*, vol. 7, no. 5, pp. 5–11, Sep. 2010, doi: 10.5120/1161-1459.

[8] A. Wulan, R. Rahman, and Desvi, "Security analysis of the VoIP (Voice Over Internet Protocol) system," *International Journal of Smart Systems*, vol. 1, no. 3, pp. 105–116, Aug. 2023, doi: 10.63876/ijss.v1i3.69.

[9] M. T.-T. Yong, S.-B. Ho, and C.-H. Tan, "Migraine generative artificial intelligence based on mobile personalized healthcare," *Journal of Informatics and Web Engineering*, vol. 4, no. 1, pp. 275, Feb. 2025, doi: 10.33093/jiwe.2025.4.1.20.

[10] O. Youness, "Secure and efficient authentication scheme for VoIP communications," *IJCI. International Journal of Computers and Information*, vol. 0, no. 0, pp. 0–0, Sep. 2023, doi: 10.21608/ijci.2023.236399.1142.

[11] R. Laurens, E. Christianto, B. Caulkins, and C. C. Zou, "Side-channel voip profiling attack against customer service automated phone system," in *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, Rio de Janeiro, Brazil: IEEE, pp. 6091–6096, Dec. 2022, doi: 10.1109/GLOBECOM48099.2022.10001537.

[12] J. C. Pang, F. Y. Lee, L. H. Chin, P. L. Ng, and S. Y. Te, "Developing work aspiration in students with learning disabilities in malaysia," *Asia Pacific Journal of Educators and Education,* vol. 40, no. 1, 299–316, 2025, doi: 10.21315/apjee2025.40.1.15.

[13] W. C. Kong, R. Parthasarathy, and L. F. Yee, "Issues surrounding private university student data privacy, security and policy management," In: *Bhateja, V., Abdul Hameed, V., Udgata, S.K., Azar, A.T. (eds) Innovations in Communication Networks: Sustainability for Societal and Industrial Impact. ICDECT 2024*. Lecture Notes in Networks and Systems, vol 1365. Springer, Singapore, 2025, doi: 10.1007/978-981-96-5223-5_34.

[14] T. Bilot, N. E. Madhoun, K. A. Agha, and A. Zouaoui, "Graph neural networks for intrusion detection: A survey," *IEEE Access*, vol. 11, pp. 49114–49139, 2023, doi: 10.1109/ACCESS.2023.3275789.

[15] Z. Azam, Md. M. Islam, and M. N. Huda, "Comparative analysis of intrusion detection systems and machine learning-based model analysis through decision tree," *IEEE Access*, vol. 11, pp. 80348–80391, 2023, doi: 10.1109/ACCESS.2023.3296444.

[16] Z. Li, W. Fang, C. Zhu, G. Song, and W. Zhang, "Toward deep learning based intrusion detection system: A survey," in *Proceedings of the 2024 6th International Conference on Big Data Engineering*, Xining China: ACM, pp. 25–32, Jul. 2024, doi: 10.1145/3688574.3688578.

[17] A. H. Ali *et al.*, "Unveiling machine learning strategies and considerations in intrusion detection systems: A comprehensive survey," *Frontiers in Computer Science*, vol. 6, pp. 1387354, Jun. 2024, doi: 10.3389/fcomp.2024.1387354.

[18] L. Diana, P. Dini, and D. Paolini, "Overview on intrusion detection systems for computers networking security," *Computers*, vol. 14, no. 3, pp. 87, Mar. 2025, doi: 10.3390/computers14030087.

[19] M. M. Rahman, S. A. Shakil, and M. R. Mustakim, "A survey on intrusion detection system in IoT networks," *Cyber Security and Applications*, vol. 3, pp. 100082, Dec. 2025, doi: 10.1016/j.csa.2024.100082.

[20] A. Pinto, L.-C. Herrera, Y. Donoso, and J. A. Gutierrez, "Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure," *Sensors*, vol. 23, no. 5, pp. 2415, Feb. 2023, doi: 10.3390/s23052415.

[21] N. Khan, K. Ahmad, A. A. Tamimi, M. M. Alani, A. Bermak, and I. Khalil, "Explainable AI-based intrusion detection system for industry 5.0: An overview of the literature, associated challenges, the existing solutions, and potential research directions," *arXiv*, 2024, doi: 10.48550/ARXIV.2408.03335.

[22] X. Zhao, K. W. Fok, and V. L. L. Thing, "Enhancing network intrusion detection performance using generative adversarial networks," 2*arXiv*, 024, doi: 10.48550/ARXIV.2404.07464.

[23] V. S. R. Pavan Kumar Neeli and V. R. G. Nallagattla, "Leveraging machine learning techniques for intrusion detection system using UNSW-NB15 dataset," in *2025 IEEE 2nd International Conference on Green Industrial Electronics and Sustainable Technologies (GIEST)*, Jamshedpur, India: IEEE, pp. 1–6, Oct. 2025, doi: 10.1109/GIEST66547.2025.11387588.

[24] Y.-S. Wu, V. Apte, S. Bagchi, S. Garg, and N. Singh, "Intrusion detection in voice over IP environments," *International Journal of Information Security*, vol. 8, no. 3, pp. 153–172, Jun. 2009, doi: 10.1007/s10207-008-0071-0.

[25] E. Anaam, S.-C. Haw, K.-W. Ng, N. Palanichamy, and J. Jayaram, "Applying fuzzy algorithm for new hybrid recommendation system in cybersecurity," pp. 030002, Online, 2025, doi: 10.1063/5.0299249.

[26] O. H. Abdulganiyu, T. Ait Tchakoucht, and Y. K. Saheed, "A systematic literature review for network Intrusion Detection System (IDS)," *International Journal of Information Security*, vol. 22, no. 5, pp. 1125–1162, Oct. 2023, doi: 10.1007/s10207-023-00682-2.

[27] I. Syllaidopoulos, K. S. Ntalianis, and I. Salmon, "A comprehensive survey on AI in counter-terrorism and cybersecurity: Challenges and ethical dimensions," *IEEE Access*, vol. 13, pp. 91740–91764, 2025, doi: 10.1109/ACCESS.2025.3572348.

[28] K. Achuthan, S. Ramanathan, S. Srinivas, and R. Raman, "Advancing cybersecurity and privacy with artificial intelligence: Current trends and future research directions," *Frontiers Big Data*, vol. 7, pp. 1497535, Dec. 2024, doi: 10.3389/fdata.2024.1497535.

[29] O. Aslan, S. S. Aktug, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics*, vol. 12, no. 6, pp. 1333, Mar. 2023, doi: 10.3390/electronics12061333.

[30] J. Zhang *et al.*, "When LLMs meet cybersecurity: A systematic literature review," *arXiv*, 2024, doi: 10.48550/ARXIV.2405.03644.

[31] H. Xu *et al.*, "Large Language Models for cyber security: A systematic literature review," *arXiv*, 2024, doi: 10.48550/ARXIV.2405.04760.

[32] F. Cremer *et al.*, "Cyber risk and cybersecurity: A systematic review of data availability," *The Geneva Papers on Risk and Insurance - Issues and Practice*, vol. 47, no. 3, pp. 698–736, Jul. 2022, doi: 10.1057/s41288-022-00266-6.

[33] M. I. B. Hanafiah *et. al.*, "TSM-NIDS: A time-series mixer-based intrusion detection system for IoT networks," *MethodsX*, vol. 16, pp. 103885, Jun. 2026, doi: 10.1016/j.mex.2026.103885.

[34] D. P. F. Moller, "Cybersecurity in digital transformation," in *Guide to Cybersecurity in Digital Transformation*, vol. 103, Cham: Springer Nature Switzerland, pp. 1–70, 2023, doi: 10.1007/978-3-031-26845-8_1.

BIOGRAPHIES OF AUTHORS

	Aizam Nazmien Alinoordin is a final year undergraduate of Bachelor of Computer Science (Honours) in the Faculty of Computing and Informatics, Multimedia University. His research focuses on intrusion detection systems, particularly hybrid approaches combining signature-based and anomaly-based techniques for securing Voice over IP (VoIP) networks. His specialization includes cybersecurity. He can be contacted at email: aizamcareer@gmail.com.
	Liana Ameerah Rosli is a lecturer at Multimedia University. She received her master's degree in computer science from Universiti Kuala Lumpur, Malaysia, and teaches Computer Science at Multimedia University, Cyberjaya, Malaysia. Her main research interests include container security, scanning, vulnerability detection, Clair, Trivy, cryptographic signing, software security, and threat mitigation. She can be contacted at email: liana.ameerah@mmu.edu.my.
	Sin-Ban Ho is an Associate Professor in Multimedia University. He received his PhD degree in information technology from the Multimedia University, Cyberjaya, Malaysia, and teaches Computer Science at Multimedia University, Cyberjaya, Malaysia. His research interests include health informatics, empirical research approach, computer education, and patterns. He is a senior member of the IEEE, IEEE Computer Society, and IEEE Education Society. He can be contacted at email: sbho@mmu.edu.my.

	Said Suleiman Naseer Al Harthy is the Director of Information and Communication Technology at Modern College of Business and Science (MCBS), Muscat, Oman. He received his master's in Information Technology from University of Wolverhampton, England, United Kingdom, and a Bachelor's in Computer Applications from Bangalore University, India. His research interests include ERP optimization and emerging technologies in higher education. He can be contacted at email: said@mcbs.edu.om.
	Ian Chai is an Associate Professor in Multimedia University. He received his PhD degree in computer science from the University of Illinois at Urbana-Champaign, USA, and teaches Computer Science at Multimedia University, Cyberjaya, Malaysia. He has worked in Connecticut and Germany. His research interests include computer science education, design patterns, health informatics, and open-sourced software. He can be contacted at email: ianchai@mmu.edu.my.