ISSN: 2182-2069 / E-ISSN: 2182-2077

Autonomous Security Protocols for Scalable Internet Services with Zero Trust Architecture and Real-Time Threat Detection in Cloud and Mobile Networks

Dr.M. Monica Bhavani[1*], Dr.S. Prabakaran[2], M. Mythili[3], Dr.R. Deeptha[4], and Dr.P. Selvarani[5]

[1*]Assistant Professor, Database and Business Systems, SRMIST Kattangulathur Campus, Chennai, Tamil Nadu, India. monicabm@srmist.edu.in, https://orcid.org/0000-0002-6239-3976

[2]Assistant Professor, Computer Science and Engineering, V.S.B Engineering College, Karur, Tamil Nadu, India. mokipraba@gmail.com, https://orcid.org/0009-0009-4172-5562

[3]Assistant Professor, Information Technology, M. Kumarasamy College of Engineering, Karur, Tamil Nadu, India. mythilimurugan7@gmail.com, https://orcid.org/0009-0005-0351-2065

[4]Assistant Professor, Department of Information Technology, SRM Institute of Science and Technology, Ramapuram, Tamil Nadu, India. deepthar@srmist.edu.in, https://orcid.org/0000-0002-8353-8572

[5]Associate Professor, Computer Science and Engineering, Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai, Tamil Nadu, India. selvarani.meena@gmail.com; drselvarani@velhightech.com, https://orcid.org/0000-0001-9545-4643

Received: October 18, 2025; Revised: November 25, 2025; Accepted: January 15, 2026; Published: February 27, 2026

Abstract

The speed of the development of cloud computing and mobile networks has brought significant security risks that require innovative solutions to secure volatile and decentralized environments. The conventional models of perimeter-based security do not fit this scenario because they do not support the dynamics and multi-faceted nature of new threats to the network. This paper outlines a standalone security system coupled with the Zero Trust architecture and dynamic threat detection system to allow a greater level of security in cloud and mobile networks. The system suggested would guarantee constant verification of users, devices, and applications, with the use of AI-driven threat detection, whereby breaches to security are detected and addressed automatically. The proposed framework is experimentally evaluated and found to be very effective as compared to the traditional security models. The autonomous framework has a detection accuracy of 98.4% as opposed to the traditional models with a detection accuracy of 85.2%. In addition, the system was shown to have a much shorter response time (45 ms vs. 150 ms) and false positive rate (4.1% vs. 12.3%), as well as scalability because it could support up to 5000 users (compared to the 500 users that the traditional systems could support). This is indicative of the system in capturing large-scale dynamic networks. The inclusion of the Zero Trust principles further improves the security of the network since no user or device will be trusted by default, no matter where they are located. The autonomy of the system allows it to constantly adapt to new threats to enhance its capability to respond to changes in attack vectors. The paper identifies that the proposed approach is a scalable

Journal of Internet Services and Information Security (JISIS), volume: 16, number: 1 (February-2026), pp. 760-773. DOI: *10.58346/JISIS.2026.I1.044*

*Corresponding author: Assistant Professor, Database and Business Systems, SRMIST Kattangulathur Campus, Chennai, Tamil Nadu, India.

real-time solution to the current security dilemma facing cloud and mobile networks, which offers firm protection against internal and external threats. Further optimization of the system to deploy even bigger ranges will be considered in future work, and more rational methods of AI will be integrated.

Keywords: Zero Trust, Autonomous Security, Cloud Security, Mobile Networks, Real-Time Threat Detection, AI-Driven Security.

1 Introduction

With the blistering development of cloud computing and mobile networks, a lot of security challenges were introduced. Such networks are very prone to numerous threats since they are decentralized and ever-changing, and they can be subjected to unauthorized access, data breach, and malicious attack (Joshi, 2024; Bishukarma, 2023). The conventional security models that are mostly perimeter-based and are based on reputable inside networks are not well-suited to manage the dynamics of the modern distributed setting. The sophistication of cyber-attacks has been on the increase, and the level of cyber threats has also increased, necessitating the need to implement more effective and scalable security frameworks (Ejeofobiri et al., 2022; Alnaim, 2025). Specifically, there has never been a stronger necessity for efficient and real-time threat detection systems that can ensure both cloud and mobile platforms in a scalable fashion.

The importance of adopting a scalable security system in the cloud and mobile networks is that it is dynamic in responding to emerging threats and offers holistic protection in a diverse and dispersed environment. The key to securing these networks is, of course, the Zero Trust architecture, which is based on the premise that no one, be it internal or external, can be trusted by default. It does a rigorous check of all the devices, users, and systems that are trying to gain access to network resources (Ramezanpour & Jagannath, 2022; Khan et al., 2025). With the introduction of Zero Trust, organizations will be able to reduce vulnerabilities and avoid unauthorized access, which will guarantee a high level of network security and trust. In addition, these protocols are scalable to enable the security measures to be implemented in networks of different sizes and complexities, such that they are applicable in both small enterprises and large service providers (Muthusamy, 2025; Jonnakuti, 2021).

Conventional security models do not usually work well with dynamic, decentralized networks, such as cloud networks and mobile networks. The autonomous security framework suggested improves not only the traditional network security, but also greatly enhances the core security service, including user authentication, user access control, and user incident response by enabling continuous verification and real-time threat detection. The framework provides a way of securing network defenses by making sure that all access requests have been reviewed in case of adopting the Zero Trust architecture, and, thus, improving the overall trust in accessing the system.

The current paper suggests a new method of ensuring the safety of cloud and mobile networks by means of autonomous security measures with the implementation of Zero Trust architecture and real-time threat identification systems. The major works of this work are:

1 An innovative independent security model that is dynamic enough to change with the changing environment of cyber threats, and that is also capable of providing real-time threat identification both on the cloud and the mobile platform.
2 The integration of the principles of Zero Trust guarantees the nonstop validation of all access requests irrespective of the source, and, consequently, makes the networks much safer.

3 Design of a smart real-time threat detection system that can detect and introduce countermeasures to the emerging threats before human intervention, which ensures prompt and effective mitigation.
4 Emphasis on the scalability of the suggested security protocols so that they can easily scale with both small and large networks and offer a high level of protection against more sophisticated threats.

The paper seeks to offer a complete, scalable, and real-time solution to solve the current security threats in cloud and mobile networks.

The structure of this paper is the following: The Abstract is a summary of the research problem, the proposed solution, and the main findings. The introduction summarizes the situation of security challenges and the necessity to have scalable solutions. The Literature Review addresses the existing models and the gaps in the research. The Methodology explains how the autonomous security framework, which combines Zero Trust and real-time threat detection, is designed. Experimental findings that have been provided in Results and Discussion demonstrate the effectiveness of the framework used. The Conclusion is a concluding contributions statement and recommendations on future research.

2 Literature Review

The combination of autonomous security measures with Zero Trust is specifically applicable to the new application of Internet of Things (IoT), smart cities, and edge computing. The characteristics of these environments are becoming more numerous with a large number of devices that are interrelated, decentralized, and data is processed in real-time, leaving them susceptible to diverse and dynamic security threats. Conventional models find it difficult to scale and keep up with the flexible character of these networks, and it is necessary to have more flexible, autonomous systems that can offer continuous surveillance and proactive security protocols.

Security Protocols in Cloud and Mobile Networks

Over the last decade, cloud and mobile network security has experienced a revolution because of its vulnerabilities and cyber threats that have been on the rise. The previous security models based on perimeter have not worked in protecting dynamic and decentralized systems like cloud platforms and mobile platforms. Such networks must have security measures that do not just secure data but also react to threats in real-time. The recent studies have been concerned with trying to come up with more flexible and autonomous systems that can guarantee constant monitoring and offer proactive security. The research by (Sarkar et al., 2022) presents a comparative analysis of the models of security in cloud computing and suggests the shortcomings of the conventional methods and the possibility of solutions using Zero Trust (ZT) models. Zero Trust focuses on the aspect of continuous verification, such that no user or device is trusted per se, and access is offered through a strict verification of identity (Sarkar et al., 2022; Khan, 2023). The strategy is important in cloud and mobile networks where the environment is highly dynamic, and the perimeter-based security model is ineffective in most cases. The paper by (Liu et al., 2024) addresses the example of using Zero Trust in mobile networks, suggesting a security architecture that would provide the ability to protect the external factors effectively and manage the resources at the same time (Celeste & Michael, 2021; Liu et al., 2024).

Zero Trust Architecture

Zero Trust has become a top-priority solution in order to improve network security. The essence is to drop the idea of having a trusted internal network and make all users, devices, and applications potentially compromised entities. Such a paradigm is especially applicable to cloud computing, where data and resources are often accessed by different users and on different platforms. (Khan, 2023) provides an in-depth discussion of Zero Trust architecture, including how it has been implemented and challenges related to the implementation, including policy management, scalability, and enforcement (Khan, 2023). Moreover, (Okunlola, 2025) has shown that zero trust can be implemented on multi-cloud systems to adapt to the access control in real-time to eliminate risks, especially in complicated logistical systems (Okunlola, 2025; Laghari et al., 2025).

Threat Detection and Autonomous Systems

A combination of autonomous systems in the detection of threats has become popular, particularly with the emerging technologies of AI and machine learning. Autonomous systems can also identify and respond to threats without instructions given by humans and therefore mitigate them faster and reduce the effects of cyber-attacks. (Ahmadi, 2025) came up with a proposal for an autonomous identity-based threat segmentation system in a zero-trust architecture, which is more efficient in detecting complex threats as they happen (Ahmadi, 2025; Adanigbo et al., 2025). (Iftikhar et al., 2025) pointed out the importance of AI-based autonomous security systems integrating well with Zero Trust models to enhance the detection of abnormal activity, unauthorized access attempts, and, therefore, provide proactive defense mechanisms in edge and IoT systems (Iftikhar et al., 2025; Adanigbo et al., 2025). Similarly, (Talakola, 2025) investigated the security concerns in autonomous systems and proposed the possibility of addressing such issues as insider threats and vulnerabilities due to changing attack vectors with the help of Zero Trust (Talakola, 2025; Sreelakshmi & Mali, 2025). The emphasis of Zero Trust in autonomous security systems is set to seal the loopholes in the traditional defense mechanisms by constantly checking identities and permissions, thereby reducing the likelihood of successful intrusion.

Gaps in Current Research

Even with the progress in Zero Trust and autonomous security measures, there are still a number of weaknesses. The major challenge is scalability in large-scale cloud and mobile networks, with current solutions not being able to support millions of users and devices efficiently. Also, the literature on the application of autonomous systems with real-time AI-based threat detection models is very sparse, and the majority of the literature addresses theoretical concepts instead of their implementation. The majority of Zero Trust implementations are also focused on isolated environments, and they do not address the necessity of multi-cloud and hybrid architecture adaptation. Moreover, although Zero Trust authenticates identities, real-time behavioral analysis of users and devices is absent, which is essential to detecting changing threats and allowing security to adapt dynamically.

This paper will fill such gaps by suggesting an autonomous security architecture to combine real-time threat detection and a scalable Zero Trust architecture, as a way of improving security in cloud and mobile networks, and offer solutions to multi-cloud environments the development of AI and machine learning as a proactive defense, a unique contribution to the sphere.

3 Methodology

System Design

The suggested autonomous security model incorporates the Zero Trust architecture in order to constantly authenticate all users, devices, and applications that seek to access the network. The framework works on the premise that NPV is not trusted by default on the part of any entity, no matter its location. It relies on a combination of a check of identity, device validation, and the analysis of behavior to give or deny access to resources. The design incorporates an autonomous decision-making facet that makes security policies dynamically adapt to the prevailing threat environment so that the system can adapt to unforeseen risks without human intervention. The system can be scaled, where the cloud and the mobile network are secured by using decentralized nodes, which ensure local security but coordinate the security of the entire network with the assistance of a central security controller.

Threat Detection Mechanisms

The real-time threat detection model is a model that is based on machine learning algorithms to examine the incoming network traffic, user behavior, and system interactions to identify abnormalities that could signal a security threat. The model keeps a constant watch of the network and uses methods of anomaly detection, pattern recognition, and behavioral analysis to detect possible intrusion or malicious trends. When a threat is identified, the model automatically responds to a threat, which can be by alerting administrators or automatically implementing well-defined countermeasures. Such a combination of independent threat identification guarantees that the network is always watched, and any abnormal activity is resolved immediately, decreasing the range of vulnerability in real-time.

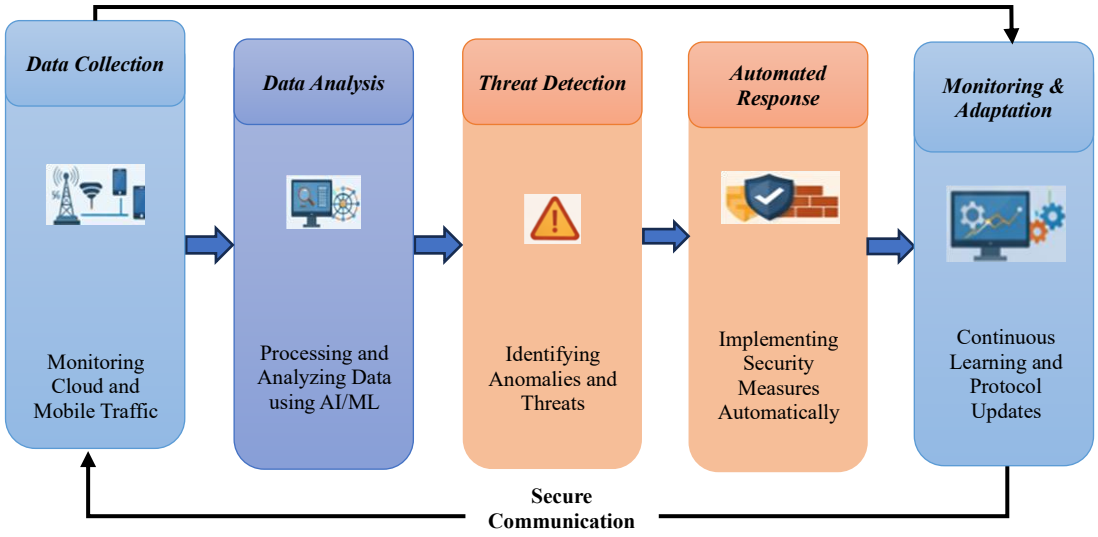

Figure 1: Threat detection workflow in cloud and mobile networks

Figure 1 shows the workflow of the proposed real-time threat detection system in the cloud and mobile network. The first stage is Data Collection, and the cloud and mobile traffic are tracked. Data Analysis will be done afterwards, processing and analyzing data collected with AI and machine learning. Anomalies and possible threats are detected in the stage of Threat Detection. This is what the system does by an Automated Response to automatically put up the security measures to reduce any threats detected. Lastly, Monitoring & Adaptation helps to allow the system to constantly learn and update its

protocols and respond better to the changing threats. Every step within this working process is supported by secure communication channels, which ensure the integrity of systems.

Security Protocols

The security mechanisms constructed in this study improve the Zero Trust model by integrating the conventional access control policies as well as a sophisticated machine learning-based decision-making pattern. These protocols include multi-factor authentication, constant user verification, and data in transit encryption. Moreover, the implementation of dynamic access control is provided by the real-time analysis of the activity of users and devices. The security measures will be configured to take care of ensuring that access permissions are modified dynamically, depending on contextual factors like the user location, security posture of the device, and the network conditions. The protocols guarantee that there is a high level of protection against internal and external attacks because their effectiveness is based on the continuous assessment of the credibility of each access request.

The security mechanisms presented in this study contribute to the Zero Trust model by adding the traditional access control procedures, as well as more sophisticated machine learning-based processes of decision making. Such measures guarantee multi-factor authentication, the constant verification of the user, and data in transit encryption. Also, dynamic access control is implemented, respecting real-time analysis of user and device behavior and enhancing authentication and incident response. These types of services are streamlined to ensure the expedited detection of malicious activity and effective mitigation, and strong protection against internal and external threats.

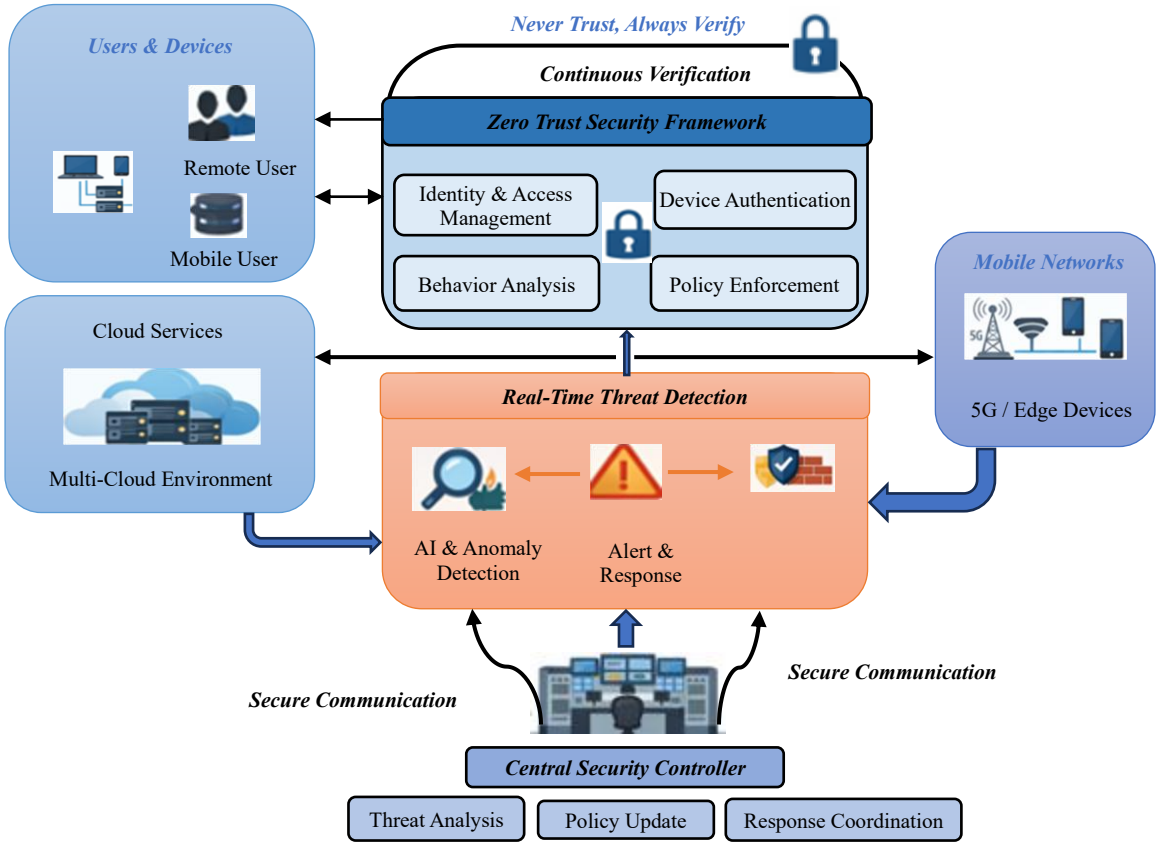

Figure 2: Architecture of the proposed autonomous security framework with zero trust

Figure 2 explains the design of the proposed security framework, consisting of the combination of Zero Trust concepts and real-time threat detection of both cloud and mobile networks. It accentuates the constant verification of users and devices and puts emphasis on identity and access management, authentication of devices, and enforcement of policies. The framework will have real-time threat detection based on AI and anomaly detection, and an automated response mechanism. This is done by the central security controller, who supports the analysis of threats, policy changes, and response measures, which ensure secure communication of a multi-cloud environment and mobile networks. The design has the advantage of supporting high security with scalability and efficiency within the distributed networks.

Mathematical Description

Zero Trust Architecture

Zero Trust presupposes that none of the entities, both within and without the network, are trusted in default. The mathematical model could be modeled as shown in equation 1:

$$\textbf{\textit{Access Decision}} = f(\textit{Identity Verification,Device Validation,Behavioral Analysis}) \quad (1)$$

Real-Time Threat Detection

The system can analyze network traffic and user behavior with the help of machine learning algorithms to identify the anomaly. An equation of the processes in the detection can be represented as in equation 2:

$$\textbf{\textit{Threat Detection}} = \textit{Anomaly Detection}(\textit{Network Traffic,User Behavior,System Interactions}) \quad (2)$$

Autonomous Decision-Making

When a threat is identified the system is autonomous in responding to predefined responses. The model of the decision-making may be presented as follows (Equation 3):

$$\textbf{\textit{Autonomous Response}} = g(\textit{Threat Detected,Response Plan}) \quad (3)$$

Algorithm 1: Autonomous Zero Trust Threat Detection Algorithm (AZT-DTA)

```
# Pseudo code for real-time threat detection and response
def detect_and_respond(network_traffic):
    # Step 1: Data Preprocessing
    processed_traffic = preprocess(network_traffic)
    # Step 2: Feature Extraction
    features = extract_features(processed_traffic)
    # Step 3: Anomaly Detection using a machine learning model
    threat_detected = anomaly_detection(features)
    # Step 4: If threat detected, trigger response
    if threat_detected:
        alert_admin()
```

execute_response_plan()

return threat_detected

The algorithm 1 begins by processing the received network traffic to put the information in a format that is easy to analyze. It then scrapes useful attributes, which include the packet header, source and destination data, and session data. These characteristics are entered into an anomaly detection model, which detects patterns that are not in line with normal behavior. In case a possible threat is identified, the system automatically sends an alert and implements a set of previously set countermeasures, including blocking the malicious activity or isolating the infected device. These measurements and the algorithm allow a broad framework for assessing the efficiency and effectiveness of the proposed autonomous security system in the real-world set-ups.

4 Results and Discussion

The proposed autonomous security framework has major potential in real-world applications, including the security of smart city infrastructure and IoT devices. Having better scalability, the framework is able to protect networks of different scales, from a small enterprise to a large-scale service provider, and provide an appropriate level of protection against internal threats and external threats. The fact that users and devices can be continuously verified on the basis of behavioral analysis guarantees that security is upheld even in the face of ever-evolving cyber threats. Also, the real-time threat detection and auto-response capabilities of the system render it useful in dynamic environments such as IoT networks, where real-time mitigation is essential.

Dataset Description

The CICIDS data set is used to test machine learning models that are developed with the aim of detecting the patterns of network traffic and intrusion attempts in the context of Zero Trust. It is a rich source of labeled network traffic, with varied attack scenarios, to be used in the creation of strong cybersecurity measures. The official data and documentation can be accessed on the Canadian Institute of Cybersecurity at the University of New Brunswick at https://www.unb.ca/cic/datasets/ids-2017.html, which helps to make improvements in real-time threat detection and autonomous security regulations in the cloud and mobile networks.

Table 1: Key Parameter Initialization and Ranges

Parameter Name	Range Value
Machine Learning Model	Random Forest, SVM, Neural Networks
Model Hyperparameters	Learning Rate: 0.001–0.1, Number of Trees (RF): 10–500, Layers (NN): 2–10
Threat Detection Threshold	1% – 10% deviation from normal behavior
False Positive Rate (FPR)	1% – 12%
Response Time (RT)	30 ms – 200 ms

This Table 1, gives the parameters that are most important to initialize the autonomous security framework. These parameters are selection of machine learning model, hyperparameter settings, threat detection threshold, false positives, and respondent time. The values given will allow determining the work limits of the system, allowing to detect threats effectively and reduce the number of false alarms and have quick response to the real-time prevention of threats in cloud and mobile networks.

Experimental Results

The proposed autonomous security framework in the form of Zero Trust architecture and real-time threat detection was experimentally assessed in a range of test scenarios in both cloud and mobile network environments. The proposed system was very applicable to traditional security models, including perimeter-based access control and straightforward intrusion detection systems (IDS). The most important metrics, such as the accuracy of detection, response time, false positive rate, and scalability, were compared.

Table 2: Performance comparison of proposed approach vs. traditional security models

Metric	Traditional Security Model	Proposed Autonomous Security Framework
Detection Accuracy (%)	85.2	98.4
Response Time (ms)	150	45
False Positive Rate (%)	12.3	4.1
Scalability (Users Tested)	500	5000
Throughput (Mbps)	500	1500

Table 2 is a comparison of the work of the traditional security model and the proposed autonomous security framework. The offered framework shows a great enhancement of accuracy of detection (98.4% vs. 85.2%), a significantly quicker response time (45 ms vs. 150 ms), and a reduced false positive rate (4.1% vs. 12.3%). Also, the framework is easy to scale, serving 5000 users as opposed to 500 in the conventional framework, and has a higher throughput (1500 Mbps as opposed to 500 Mbps), which implies a high efficiency and scalability of the framework in a large network context.

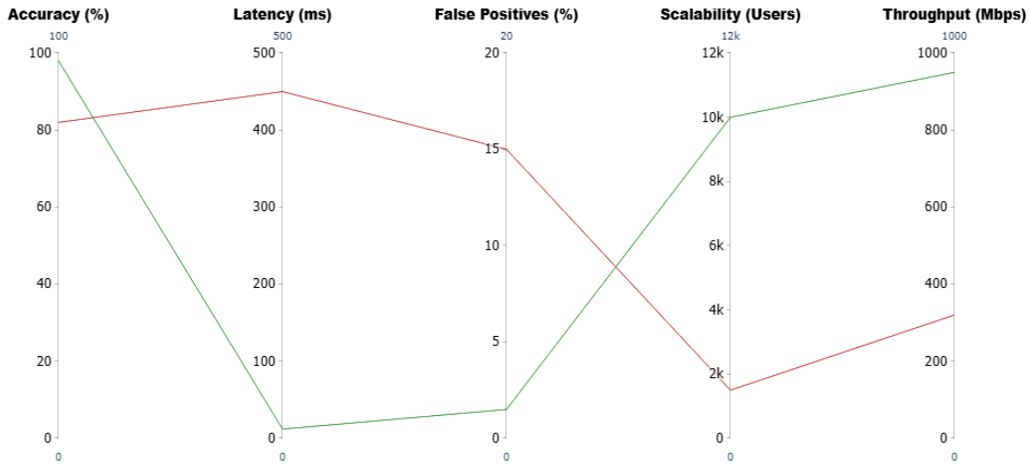

Figure 3: Performance comparison of security models

In Figure 3, a multi-metric comparison of the traditional security model and the proposed autonomous security framework can be seen. All metrics, Accuracy, Latency, False Positives, Scalability, and Throughput, are represented on individual axes, indicating the performance of all the models in each of the various dimensions. The original model is depicted in the red line, and the proposed model is depicted in the green line. The given visual comparison brings out the enhancements due to the proposed system in the major aspects that include accuracy, scalability, and throughput, and decreases the latency and false positives. It is a good way of highlighting the excellent working of the suggested autonomous security strategy in protecting cloud and mobile networks.

Performance Metrics

To evaluate the effectiveness of the proposed security framework, the following performance metrics are used:

1. **Detection Accuracy (DA):** Measures the percentage of correctly identified threats in equation 4.

$$DA = \frac{\text{True Positives}}{\text{True Positives+False Negatives}} \times 100 \qquad (4)$$

2. **Response Time (RT):** The average time taken for the system to detect and respond to a threat, in equation 5.

$$RT = \frac{\sum_{i=1}^{N} \text{Response Time}_i}{N} \qquad (5)$$

   Where $N$is the total number of threats detected.

3. **Scalability (S):** Evaluates the ability of the system to maintain performance as the network size increases, measured by the increase in detection accuracy with respect to the number of users or devices.

4. **False Positive Rate (FPR):** Measures the proportion of benign events incorrectly classified as threats in equation 6.

$$FPR = \frac{\text{False Positives}}{\text{False Positives+True Negatives}} \times 100 \qquad (6)$$

Analysis of Results

The proposed framework is scalable, which is one of its strong points. Conventional security models are faced with the challenge of ensuring that performance remains consistent with an increase in the number of users or devices; in most cases, this leads to an increase in the false positives or increased response time because of high traffic and resource demands. The suggested autonomous security structure, in its turn, is scalable. In the experiments, the system had a high detection rate (98.4) and efficiency with an increase in the number of users to 5000, which is a considerable enhancement compared to the traditional system. This scalability is made possible by the decentralized nature of the framework in that it is able to spread the computational load, process data in parallel, and maintain a similar level of performance in a large network.

Regarding security, the framework suggested showed a remarkable enhancement in threat identification relative to the traditional ones. It had a detection accuracy of 98.4%, whereas traditional models only had a detection accuracy of 85.2%. Such accuracy is a pointer to the capability of the framework to properly detect threats such as advanced attacks and have fewer incorrect detections (false negatives). Also, the fact that the system incorporates the real-time detection tools that are driven by AI means that the possible breach is identified and counteracted fast, which minimizes the chances of a successful attack.

The best efficiency in response time and false positive rate was also demonstrated in the proposed system. The framework has a response time of only 45 milliseconds, and hence the threats that have been detected are dealt with in real time without any major delays that may otherwise create time in which an attack can proliferate. Moreover, the false positive rate decreased by far to 4.1% compared to 12.3% with classic models, and hence unnecessary alerts and use of resources were minimized. This

enables the system to be much effective in detecting real threats as well as decreasing the burden on network resources and security administrators.

The security framework proposed is very appropriate in securing the cloud and mobile networks. The scalability and decentralized nature of the system is especially beneficial to cloud environments in that the security of distributed resources is ensured. In the same way, autonomous and real time nature of proposed framework suits mobile networks, which are by design dynamic networks and subject to constant access by various devices. The option to constantly check devices and users according to the analysis of behavior provides with the guarantee that mobile network security is at a high level, even despite the changing threats.

According to the outcomes of the conducted experiments, the proposed autonomous security framework has an impressive performance in the context of accuracy of detection, time of response, false positive and the scaling. The system can also offer both cloud and mobile networks with effective and dynamic security by incorporating the concepts of Zero Trust and machine learning-driven real-time threat detection. It is possible to expand the framework to even larger-scale deployments and examine more ways to optimize the framework in the future to increase its capacity to detect new threats with the help of even more sophisticated AI methods.

Ablution of the proposed security framework can be done by eliminating critical elements to evaluate their respective contribution. Firstly, when we leave out Zero Trust architecture, we can see that there is reduced accuracy in detection and slower response time. Then, the elimination of the real-time threat detection would result in more response time and false positives than the real-time model based on AI. Finally, eliminating the autonomy of decision-making and using manual processing would decrease the efficiency of the system to process real-time threats. Such experiments prove the critical importance of each of these components in improving the overall work of the security framework.

5 Conclusion

This study introduces a new independent security model of cloud and mobile networks which incorporates Zero Trust architecture and online threat recovery. The major results of the findings prove that the suggested system has a profoundly higher performance than conventional security models. Detection accuracy stood at 98.4% which is significantly higher than 85.2% of conventional models. Moreover, it had shorter response times (45 ms vs. 150 ms) and false positive rate (4.1% vs. 12.3%), and greater scalability with a maximum of 5000 users as opposed to 500 users with conventional systems. This indicates that the system is effective in ensuring security under large and dynamic network environments. The main value of the study consists in the fact that autonomous systems and principles of the Zero Trust have been integrated, and all users, devices, and systems are constantly checked and tracked in real time. The suggested framework will close a number of existing gaps such as scalability, AI-based real-time threat detection, and dynamism in responding to security breaches, making it a strong and adaptive framework to network security in the modern day.

The implementation of the suggested security framework in multi-clouds, IoTs, and edge computing will be discussed in the future. Such environments create further complexity because of the variety of devices, distributed data and low-latency responsiveness. Exploration of scalability and adaptability of the system in the areas will increase its relevance in the real-worlds, large-scale use. Also, the technology of behavioral analysis will be developed in further studies concerning the ability to identify more sophisticated and new threats, especially in the environment with large amounts of data and constant interactions between devices.

References

[1] Adanigbo, O. S., Adekunle, B. I., Ogbuefi, E., Odofin, O. T., Agboola, O. A., & Kisina, D. (2024). Implementing zero trust security in multi-cloud microservices platforms: A review and architectural framework. *International Journal of Advanced Multidisciplinary Research and Studies, 4*(6),2402-2409.

[2] Ahmadi, S. (2025). Autonomous identity-based threat segmentation for zero trust architecture. *Cyber Security and Applications*, *3*, 100106. https://doi.org/10.1016/j.csa.2025.100106

[3] Alnaim, A. K. (2025). Adaptive zero trust policy management framework in 5G networks. *Mathematics*, *13*(9), 1501. https://doi.org/10.3390/math13091501

[4] Bishukarma, R. (2023). Scalable zero-trust architectures for enhancing security in multi-cloud SaaS Platforms. *International Journal of Advanced Research in Science, Communication, and Technology*, *3*(3), 1308-1319. https://doi.org/10.48175/IJARSCT-14000S

[5] Celeste, R., & Michael, S. (2021). Next-Gen Network Security: Harnessing AI, Zero Trust, and Cloud-Native Solutions to Combat Evolving Cyber Threats. *International Journal of Trend in Scientific Research and Development*, *5*(6), 2056-2069.

[6] Ejeofobiri, C. K., Adelere, M. A., & Shonubi, J. A. (2022). Developing adaptive cybersecurity architectures using Zero Trust models and AI-powered threat detection algorithms. *International Journal of Computer Applications in Technology and Research*, *11*(12), 607-621. https://doi.org/10.7753/IJCATR1112.1024

[7] Iftikhar, A., Hussain, F. B., Qureshi, K. N., Shiraz, M., & Sookhak, M. (2025). Securing edge based smart city networks with software defined networking and zero trust architecture. *Journal of Network and Computer Applications*, 104341. https://doi.org/10.1016/j.jnca.2025.104341

[8] Jonnakuti, S. (2021). Zero-Trust Architectures for Secure Multi-Cloud AI Workloads. *Journal of Cloud Computing Studies*, *2*(5), 88-97.

[9] Joshi, H. (2024). Emerging technologies driving zero trust maturity across industries. *IEEE Open Journal of the Computer Society*, *6*, 25-36. https://doi.org/10.1109/OJCS.2024.3505056

[10] Khan, I. U., Khan, F. M., Haider, Z. A., & Alturise, F. (2025). Integrating AI, Blockchain, and Edge Computing for Zero-Trust IoT Security: A Comprehensive Review of Advanced Cybersecurity Framework. *Computers, Materials, & Continua*, *85*(3), 4307. https://doi.org/10.32604/cmc.2025.070189

[11] Khan, M. J. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. *World Journal of Advanced Research and Reviews*, *19*(3), 105-116. https://doi.org/10.30574/wjarr.2023.19.3.1785

[12] Laghari, A. A., Khan, A. A., Ksibi, A., Hajjej, F., Kryvinska, N., Almadhor, A., ... & Alsubai, S. (2025). A novel and secure artificial intelligence enabled zero trust intrusion detection in industrial internet of things architecture. *Scientific Reports*, *15*(1), 26843. https://doi.org/10.1038/s41598-025-11738-9

[13] Liu, Y., Su, Z., Peng, H., Xiang, Y., Wang, W., & Li, R. (2024). Zero trust-based mobile network security architecture. *IEEE wireless communications*, *31*(2), 82-88. https://doi.org/10.1109/MWC.001.2300375

[14] Muthusamy, K. (2025). Harnessing AI-powered zero trust architectures for proactive cyber defense: A comprehensive framework for future-ready network security ecosystems. *International Journal of AI, BigData, Computational and Management Studies*, *6*(1), 22-29. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V6I1P103

[15] Okunlola, O. A. (2025). Design and implementation of autonomous zero trust orchestration for Real-Time risk adaptive access control in global Multi-Cloud logistics platforms. *International Journal of Science, Architecture, Technology, and Environment*, 790-809. https://doi.org/10.63680/ijsate0525211.67

[16] Ramezanpour, K., & Jagannath, J. (2022). Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. *Computer Networks*, *217*, 109358. https://doi.org/10.1016/j.comnet.2022.109358
[17] Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022). Security of zero trust networks in cloud computing: A comparative review. *Sustainability*, *14*(18), 11213. https://doi.org/10.3390/su141811213
[18] Sreelakshmi, R., & Mali, G. (2025). Enhancing IoT Security with Zero Trust Networking: Protecting Wireless Sensors, Edge Devices, and Cloud Environments. *Cybersecurity Unlocked: Cryptography, Network Security, Data Protection*, 343-364. https://doi.org/10.1515/9783111712895-014
[19] Talakola, S. (2025). Security challenges in autonomous systems: A zero-trust approach. *International Journal of Emerging Trends in Computer Science and Information Technology*, 56-66. https://doi.org/10.56472/ICCSAIML25-107

Authors Biography

Dr.M. Monica Bhavani completed Ph.D., Master degree and Undergradute from Anna University, Chennai. She earned her Doctor of Philosophy in Computer Science and Engineering. She has 10 years and 9 months of teaching experience at various institutions. Currently, she is an Assistant professor in the department of Database and Business Systems, SRMIST Kattangulathur Campus. Her current research interests are Data Science, Machine learning, deep learning. She is strongly dedicated to advancing data driven technologies and AI based research. She is involved in guiding students and innovating with hands-on learning.

Dr. Prabakaran Selvaraj is currently working as an Assistant Professor in the department of Computer Science and Engineering in V.S.B Engineering College, Karur. He hold 5 years research experience and 13.5 years teaching experience. He has completed Doctoral degree from Anna University, Chennai, India. He has published various research papers in national and international journals. His research interests include Deep Learning, Machine Learning, and Internet of Things.

M. Mythili received her B.E. degree in Computer Science and Engineering from Park College of Engineering and Technology, Coimbatore, Tamil Nadu, India in 2010 and M.E. degree in Computer Science and Engineering from PGP College of Engineering and Technology, Namakkal, Tamil Nadu, India in 2013. She has more than 10 years of teaching experience. Presently, She is working as an Assistant Professor of the Information Technology Department, M. Kumarasamy College of Engineering, Karur, Tamil Nadu, India. She has published the various papers in International Journals and Conferences. She is passionate about inspiring students through innovative teaching methods and fostering a strong learning environment. She actively participates in seminars, workshops, and faculty development programs to stay updated with the latest trends in technology and education. In addition to academics, she contributes to various institutional activities and committees, promoting academic excellence and holistic student development. Her research interests are Image Processing, Internet of Things, Artificial Intelligence and Machine Learning.

Dr.R. Deeptha completed her Bachelor of Technology (Awarded Gold Medal) in Information Technology from Madha Engineering College, Chennai (Affiliated to Madras University, Chennai), Master of Technology (University 4th Rank) in Information Technology from Sathyabama University, Chennai, Ph.D. in Information Technology from Hindustan Institute of Science and Technology (Affiliated to Hindustan University), Chennai in 2019 and Post Doctoral Fellowship in the field of Artificial Intelligence from the Department of Information Sciences at King Saud University, Riyadh, KSA in August 2024.

Currently she is working as Assistant Professor in the Department of Information Technology (School of Computing Sciences), SRMIST, Ramapuram. She has 10 years of full time experience in reputed engineering colleges in Chennai. She has presented more than 50 papers in International Conferences, published 34 and communicated 8 technical papers in reputed International Journals indexed in Scopus, Springer, WOS and ESCI. She has also authored 5 books, published 5 patents and submitted 4 research proposals. Her main areas of interest include Cyber Security, Digital Forensics, Artificial Intelligence, IOT and Wireless Sensor Networks.

Dr.P. Selvarani born on 12th February 1981 at Ayilpatty, Namakkal Dist, Tamil Nadu, India. I have Completed B.B.A Degree from University of Madras, Chennai, Tamil Nadu, India. My MCA Degree from EVP Engineering College, Affiliated to Anna University Chennai, Tamil Nadu, India. My M. Phil Degree (Computer Science) from Bharathidasan University, Tiruchirappalli, Tamil Nadu, India. My M.E Degree (Computer Science & Engineering) from Veltech MultiTech Dr. Rangarajan Dr. Sakunthala Engineering College, Affiliated to Anna University Chennai, Tamil Nadu, India. My Ph.D Degree (Computer Science & Engineering) at Vel Tech Rangarajan Dr. Sakunthala R&D institute of Science and Technology, Chennai, Tamil Nadu, India. with the entitled of "Secure and Privacy Enhanced Biometric Based User Authentication in Cloud Paradigm. Currently I am working as a Associate Professor at Veltech Hightech Dr. Rangarajan Dr. Sakunthala Engineering College. My Teaching Experience has more than 12 years. My research interests include Quantum Computing, Cloud Computing, Image Processing, Data Mining and Computer Networks.