Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 20 No. 15 (2026) | OPEN ACCESS

https://doi.org/10.3991/ijim.v20i15.62594

PAPER

Real-Time Threat Detection in Mobile Networks Using an Adaptive AI-Based Firewall Framework

Sai Kiranmai Dornala[1], P. Senthil Kumar[2] (✉)

[1]BEST Innovation University, Gorantla, Andhra Pradesh, India

[2]SRM Institute of Science and Technology (Formerly SRM University), Tiruchirappalli, Tamil Nadu, India

senthilkumar.p@ist.srmtrichy.edu.in

ABSTRACT

The rapid growth of cyber landscapes and the development of a new cybersecurity model incorporating PET, deep learning, fuzzy systems, keystroke dynamic authentication, and encryption. It is used to prevent attacks by malware or unauthorized access to cloud systems. The proposed framework, which integrates an artificial intelligence (AI)-driven approach with identity and access management (IAM), enables the adaptive implementation of risk-based login authentication and real time anomaly detection. Unlike conventional security systems that depend on fixed rules and signatures, we provide more sophisticated solutions. A Floydel firewall is dynamically tailored through deep neural networks (DNNs) and automatically adjusts to fluctuating traffic patterns. It employs malware classification based on behavior, utilizes fuzzy logic to manage uncertainty during intrusions, and uses keystroke dynamics for user verification through typing patterns. The experiment demonstrates a 97.6% detection accuracy on benchmark data, while significantly reducing false positives and ensuring data confidentiality through encryption. The nature of cloud security can evolve based on the specific circumstances and threats we encounter. Looking ahead, we plan to delve into cryptography and distributed training to bolster decentralized infrastructures. This proposed framework aims to fortify data protection and ensure user privacy in essential areas like healthcare, financial services, and e-governance, thereby fostering increased trust.

KEYWORDS

dynamic firewalls, malware detection, fuzzy systems, identity and access management (IAM)

1 INTRODUCTION

With the advancement of technologies, the attack of cybercriminals is becoming more complicated and often causes severe damage to network infrastructure. Earlier, security systems detected attacks using laws and signatures. Consequently, they cannot recognize advanced and novel attacks. Consequently, smart systems are required. These systems can enhance the detection and reaction to attacks

Dornala, S. K., Senthil Kumar, P. (2026). Real-Time Threat Detection in Mobile Networks Using an Adaptive AI-Based Firewall Framework. *International Journal of Interactive Mobile Technologies (iJIM)*, 20(15), pp. 65–79. https://doi.org/10.3991/ijim.v20i15.62594

Article submitted 2026-05-09. Revision uploaded 2026-06-19. Final acceptance 2026-06-23.

in real time. Deep learning (DL) models can detect low-level anomalies in the traffic of any network that can indicate malicious use. Intelligent firewalls are security systems that work on intelligent techniques that are not modified or require any human adjustment in response to new threats and attacks. The analysis used a DL algorithm to develop a complete cybersecurity framework with optimally mobile customized artificial intelligence (AI) firewalls for real-time network threat analysis. Fuzzy systems, keystroke dynamics, and cryptographic protocols have all been used to enhance privacy. This framework represents a notable step forward in enhancing the protection of sensitive data in areas involving healthcare, financial services, and e-governance. It creates its own defense measures to foresee and put an end to new dangers before abuse. Today, organizations are adopting digital transformation. As we adopt the cloud and use smart devices, businesses will want cyber security solutions that are resilient, adaptive, and smart. This study proposes a novel concept that employs privacy-enhancing technologies, DL, fuzzy logic, keystroke dynamics authentication, and an efficient encryption protocol to formulate a dynamic AI firewall for pro-active countering threats in cloud landscapes. The main goal of this study is to implement a dynamically customized firewall programmed with deep neural networks (DNNs), which will be trained with various patterns of network behavior on an ongoing basis. Unlike static systems, the proposed firewall is dynamic because it uses AI-based identity and access management (IAM). However, this justifies its authentication using context. Real-time malware detection can be achieved using DL classifiers [1]. They analyzed data from the network traffic and system behavior. They performed better than older signature-matching approaches. Simultaneously, fuzzy logic can help the system deal with vague or incomplete indicators of threat, as often occurs with stealth attacks, along with useful probabilistic decision making [2]. Keystroke Dynamics strengthen access security by checking the unique typing patterns of users. The results showed that AI-augmented firewalls are capable of transforming threat prevention in critical sectors such as healthcare, banking, and e-governance [3]. Furthermore, the framework has a design that is scalable and future-ready, with a self-evolving architecture that updates automatically against new threats. In the future, we plan to develop quantum-resistant cryptography and federated learning models to prevent attacks from post-quantum threats. Finally, we want to draw a connection between a firewall and a next-generation cyber that results in a paradigm to ensure real-time intelligence and consistent protection of the cloud-enabled ecosystem. Figure 1 shows the dynamically customized AI firewall framework. As shown in the diagram, a dynamic firewall disallows any type of harmful incoming traffic from its network. In addition, it routes all the incoming traffic through an AI Core. The AI Core consists of four main components (e.g., Deep Learning, Fuzzy Logic Controller, Keystroke Behavior, and Quantum Safe Encryption). The elements of threat detection, behavior analytics, and secure authentication are hand-in-glove [4]. The AI Core learns and adapts on a continuous basis to protect itself against emerging threats. This creates a self-evolving system to improve detection. Intelligent processing provides the desired results in a secure network environment. This framework can be used for high-security sectors, such as healthcare, finance, and e-governance, and is future-ready through Quantum-Resistant Cryptography and integration with federated learning for decentralized model training to enhance privacy [5].

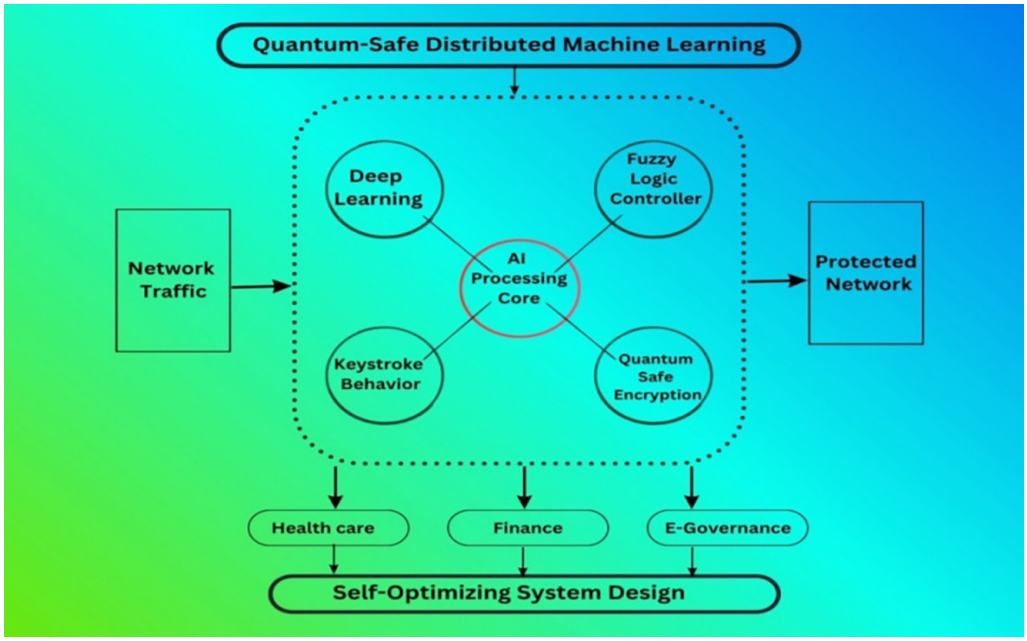

Fig. 1. Dynamically customized AI firewall framework

2 BACKGROUND

Organizations are becoming increasingly reliant on cloud effectiveness. Security measures fail to address these issues. Firewalls and intrusion detection systems are unable to detect new and evolving threats, either anymore or in real-time. They work based on signatures and are static. Today's cyberattacks are flexible and consist of polymorphic malware, zero-day attacks, and sophisticated phishing. As threats evolve, researchers and practitioners can utilize AI and machine learning (ML) to reinforce existing systems. Scientists have shown how DL algorithms can model patterns and behavior in network traffic. By amalgamating with other developing technologies such as fuzzy systems, encryption systems, and biometrics, AI can help the future of cybersecurity by means of threat prediction, context awareness, and intelligent decision-making. This study addresses critical needs in this domain by building a dynamically customized real-time AI firewall to deal with attacks in real time. The design of this system consists of a neural architecture utilizing deep learning, which picks up and adapts to varying traffic conditions over time. Thus, this neural architecture can isolate normal from abnormal behavior. With the help of fuzzy logic, the modeling manages the uncertainty that comes with unknown threat scenarios. Similarly, the keystroke dynamic authentication process represents the second level of authentication. Encryption and other technologies have also created safe and secure responses to threats.

2.1 Significance of dynamically customized firewall

The system is equipped with an understanding of how a network behaves normally owing to new data machine-training algorithms. This feature essentially evolves and closes the security gap between attack emergence and manual security or patching updates. Thus, it protects against zero-day attacks that are unknown and

breach conventional forms of security [6]. A dynamic firewall integrated with fuzzy systems, encryption, and keystroke dynamics may pave the way for a multilayered solution that can tackle the problems posed by current cyber invasions. This reduces false positives and thus helps teams perform more effectively. Hence, the teams do not have false alarms that contain real malware. This helps shorten the response times to actual threats, as they are automatically assessed and tackled. Finally, context-aware authentication enhances security by adjusting requirements based on risk. Security breaches in sensitive industries such as healthcare and finance can be cataclysmic. The framework prevents this damage while also being performant from a system and user experience perspective [7].

2.2 Scope of the research

The purpose of this study is to design and evaluate an integrated cybersecurity framework based on a dynamically customized AI firewall architecture for real-time network threat detection. The first step of this framework is to identify the weaknesses of standard static security methods. Next, it uses DL algorithms to prevent threats from being modified. We focus on cloud environments, where the increasing complexity of infrastructure and variety in access have resulted in serious security issues that cannot be effectively managed with current solutions. The university has a special room where advanced projects are available, and where they work on applications [8]. The implementation of various critical sectors, such as health, finance, and e-governance, was indirectly considered in this study. They require security because their data are sensitive. Despite the new work being better than the old work, there is still scope for further improvement. Essential factors for the dynamic cybersecurity framework. A younger generation is also emerging. The addition of quantum-resistant cryptography, along with federated learning techniques, allows for decentralized sharing of threat intelligence [9].

3 LITERATURE REVIEW

Cybersecurity has advanced rapidly, and new intelligent firewalls have been developed using ML and DL techniques to detect malware. Rule- and signature-based methods of traditional firewalls cannot detect zero-day attacks or modify malware variants. According to Sharma, an ML-based firewall can learn dynamically from network traffic patterns and detect anomalies more effectively than static-rule-based systems. Moreover, the classification accuracies of the SVM, random forest (RF), and DT models in identifying benign and malicious data packets were studied. An intelligent firewall can also deploy real-time analytics to reduce false positives and enhance detection in real time, according to some experts. Through predictive modeling and careful behavioral analysis, one can “proactively” avoid an attack before it occurs. According to Kumar and Singh, firewalls with neural networks are incorporated into proactive frameworks so that they can adapt continuously to threats and do not require any prior knowledge of malware signatures [10]. The detection of quantum algorithms is studied on-whiz, including new differentiable quantum random functions and non-effective updaters. These new designs open up possibilities for firewall designs. Quantum ML refers to this phenomenon. This increases the scalability and responsiveness of intrusion detection system. Al Qahtani launched quantum-anchored anomaly detection models based on quantum support vector machines and Grover’s algorithm to reduce training time and improve the detection rate of

encrypted and obfuscated malware traffic. Even though the current hardware is limited, simulation work has various possible applications that use quantum resilience in cybersecurity infrastructure, especially in sensitive and private sectors. Research shows that there are several ethical and regulatory issues facing quantum firewalls. When designing a system, it is essential to keep in mind data privacy, transparency in AI decision-making, and compliance governed by frameworks such as GDPR and PDPL. A recent analysis by Hasan revealed that for intelligent firewall functionality, trustworthiness and interpretability through explainable AI (XAI) are essential. Therefore, intelligent firewall solutions must be strong, explosive, and socially ethically sustainable [11]. The increasing amount of work in this area shows that security is now an all-encompassing phenomenon that is adaptive, pre-emptive, and ethical.

Table 1. Meta-analysis on intelligent firewalls and malware detection

Authors	Technique/Model	Application Area	Key Outcome and Contribution
Sharma et al.	Random Forest, SVM	AI-based Intrusion Detection	Showcased ML advantages over static firewalls
Kumar and Singh	Neural Networks, Real-time Feedback	Proactive Malware Defense	Demonstrated real-time, adaptive firewall framework
Roy and Chen (DeepRan)	BiLSTM + CRF	Early Ransomware Detection	Validated deep sequential learning for threat prediction
Al Qahtani et al.	Quantum SVM, Grover's Algorithm	Quantum Malware Detection	Explored QML for scalable, encrypted malware detection
Moujoud et al.	Hybrid ML-DL Models	Ransomware Detection Survey	Advocated hybrid approaches for enhanced accuracy
Hasan et al.	XAI	AI Firewall Decision Transparency	Addressed ethical and privacy aspects of AI firewalls

Table 1 shows that cybersecurity research has come a long way away, going from static rule-based systems to intelligent adaptive firewalls using machine learning, deep learning, and quantum computing. Research has shown that DL models, such as CNN, LSTM, and BiLSTM, can learn complex patterns in network traffic. Therefore, compared with standard algorithms, they provide high detection rates and low false-positive values. The hybrid system is reinforced through capabilities, such as fuzzy logic, real-time feedback, and behavioral biometrics.

4 PROPOSED METHODOLOGY

Figure 2 shows the novel personalized intelligent AI firewall architecture based on deep learning, fuzzy logic, keystroke dynamics, and encryption specifications presented in this study for real-time intelligent threat analysis. Over time, this evolving framework incorporates feedback, in contrast to stationary systems increasingly being developed to defend against non-advanced malicious malware and access control with the cloud. The novel, trusted dynamic customization of the firewall architecture is helpful for designing real-time network security. Different types of tools and techniques can be used to detect, analyze, and mitigate threats. The Internet Gateway tracks the traffic of users and their devices. Users can be IoT devices. The core of the dynamic AI firewall system must cooperate with the intelligence of several components. The traffic is then fed into the core. This project features a DL module that implements DNNs and performs real-time traffic analysis.

This component includes functionalities that discover patterns and deviations and indicate malicious behavior such as ransomware, phishing, and DDos attacks [12]. Detection always improves the learning of a behavioral signature for a new event. It does not create rules using metrics for new events. We can use a fuzzy logic system to represent a case that may be doubtful but does not cause damage. This factor places threats on context. As a result, fewer false positives were obtained. The software determines the difference between the actual security events and good anomalies. For instance, failed logins do not increase the number of red flags. Through your Projected Network Environment, you can view the network [13]. A firewall can project how far the threat will spread and where weak links might be available for exploitation. The system will enable defense against threats before they occur. In addition, Keystroke Dynamics are essential for the authentication and safeguarding of data. It then gathers information from users based on the timing and pattern of the keystrokes. When data are communicated and stored, AES, TLS, and other protocols are used to secure them. The computer collection gathers information from various components and utilizes this information to realistically limit system security responses. This includes dynamically changing the firewall rules. The risk scores help in decision-making, which means that the system will take stricter actions when there are heightened risks but will not disrupt legitimate activity at such times. A feedback loop for continuous learning is a major innovation in this architecture, which enables the system to become matter and smarter based on experience. The loop continuously updates deep-learning models with newly discovered threat patterns. Additionally, adjustments to the fuzzy logic rules were made during the past risk assessments. In addition, keystroke dynamics thresholds have been optimized [14, 15], and firewalls not only stop off known attacks. Additionally, they can predict and adapt to new attacks. The model uses a method with many layers that employs DL and behavioral biometrics, as well as encryption and probabilistic reasoning. Cloud systems, the IoT, and enterprise networks can also be used. For instance, when a user logs in, the initial authentication occurs through the keystroke dynamics of the user. When a user's activity sets off an anomaly notification from a DL module, the fuzzy system assesses the user's behavior. In the end, it provides a probability of, for example, 0.85 or 85% of getting a malware attack. The decision engine prevents this connection and records events. Moreover, it is fed back into the learning loop. Therefore, future detection methods should be improved. A significant advancement in smart network security is the comprehensive and iterative approach [16]. The proposed novel security framework uses fuzzy logic, along with recently advanced technology, keystroke dynamics, and encryption technologies using CNN-LSTM and other modern technologies. With this multilayer system, it is possible to obtain a clearer view of the 2-dimensional structures of complex traffic patterns that are not easily detectable. It is particularly effective for identifying new security threats and changing virus programs. The use of fuzzy logic to evaluate threats is a significant development. Fuzzy logic works not only with true or false logic; instead, it examines the odds of a true threat. Consequently, fuzzy logic is efficient in minimizing false positives. Another level of credential verification to prevent identity from being misused is added through the use of behavioral biometrics with keystroke dynamics. When a firewall presents a feedback loop, it ensures that it is self-learning and can cope with new threats. Furthermore, it reduced the response time to zero. The decision engine enhances performance by intelligently allocating resources according to risk [17]. However, this methodology requires several technical and practical aspects. The DL section particularly uses CNN-LSTM models and may require high-performance computing using GPU and TPU when there is dense network traffic. The training data must be decent, plentiful, and varied for the

models to be effective. Consequently, it must encompass a broad range of benign and malicious traffic patterns for effective generalization. The membership functions and rule set must be calibrated or tuned such that they have the right proportions with respect to security sensitivity and user friendliness. The system must embrace cloud-native principles to support horizontal scaling and must be able to withstand loads of various sizes. In addition, PDPL, GDPR, and HIPAA mandated that global and regional data protection laws need privacy-enhancing technologies (PETs) to be built on the right through the entire process. The sound growth of dynamically customized AI firewall systems was considered for implementation [18].

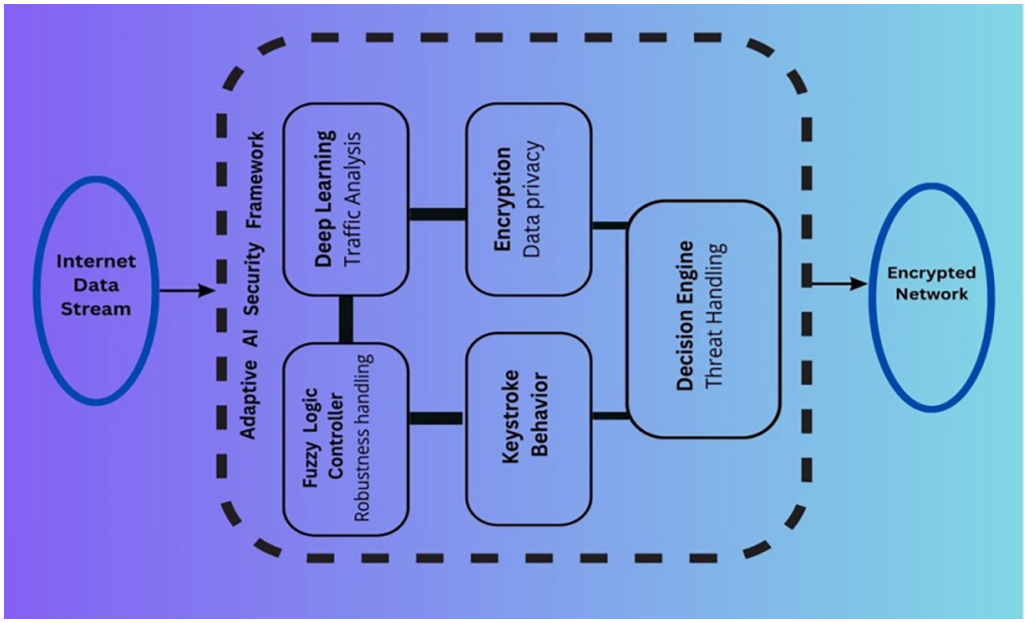

Fig. 2. Dynamically customized AI firewall architecture

4.1 Implementation of the dynamically customized AI firewall

The development of a dynamically customized AI firewall utilizes intelligent network security based on DL, fuzzy logic, behavioral biometrics, and encryption. This development is an important milestone in network security and firewall technology [19]. Traffic analysis is the first step in which packets captured on a net are subjected to an anomaly detection algorithm based on DL. It assesses an anomaly score and identifies known attacks by comparing packets with a large collection of attack signatures. If the user is required to authenticate at the same time, keystroke dynamics behavior verification is invoked through dwell and flight times with regard to the stored user profile. The fuzzy threat evaluation module calculates the overall threat probability based on the source reputation, time of access, user authenticated status, and destination sensitivity. When a threat is identified, virtual simulation studies the possible spread and damage in the network. The engine generates a risk score to decide whether to block, quarantine, monitor, or allow. The firewall dynamically chooses the AED-256/AES-128/TLS encryption schemes based on sensitive data [20]. Data were either forwarded or blocked in this manner. The interactions were noted in order to understand and modify the user's knowledge. Periodic model upgrades were performed for the threat patterns, fuzzy rules, and user profiles. The feedback loop helps the system to change automatically without manual changes from the new threat. When you first set up your firewall, it will come with

the patterns used to launch the attacks. Additionally, there are user profiles, encryption keys, and fuzzy rules. The modules work together to enforce risk-aware and privacy-compliant security policies in real time, making the firewall intelligent and resilient against modern attacks [21]. The proposed system described in this section is an example of a fully customizable dynamic AI firewall that protects the network infrastructure. The AI Firewall analyzes the incoming packets into the network using a multi-level (or layered) process. The first layer consists of DL-based anomaly detection, which identifies packet characteristics and assigns weighted anomaly scores and identifies signature patterns of known attacks. If authentication is needed, the AI Firewall uses behavioral biometric methods based on keystroke dynamics analysis and compares the dwell time and flight time of the keystrokes to the stored user profile so as to authenticate the user to the configurable similarity threshold.

5 RESULTS AND DISCUSSION

5.1 Dataset description and preparation

The evaluation of the effectiveness of our dynamically customized AI firewall combines standard benchmark datasets with synthetically generated network traffic to form a hybrid one [22, 23]. The NSL–KDD dataset was used, as well as a ransomware traffic dataset built from various datasets. A large amount of malware can perform a variety of malicious and non-malicious behaviors, such as DDoS, ransomware, unauthorized access, and data exfiltration. The dataset prepared by the company strictly optimized the performance of the AI model. They selected features, such as packet headers, protocol details, payload signatures, and timing indicators. We adjusted these to ensure that the input scales for all features were similar. To enhance the ability of the model to adapt to varying real-life traffic situations, synthetic samples were generated using variational data augmentation. Using up-sampling and down-sampling, the model was able to learn different types of attacks. In simpler terms, dominant classes were low-sampled, and under-attack classes were oversampled. Therefore, the model was not favored for frequent classes during the training. AI firewalls are becoming more popular among businesses and companies; they are believed to handle complex cyber threats and solve problems, such as ransomware. To train and validate the deep learning, fuzzy logic, and behavioral analysis of AI firewalls, this dataset was developed.

5.2 Detection accuracy and precision

Table 2 indicates that the dynamically customized AI firewall achieved a high accuracy of 97.6% against various types of attacks. Instead of lying in the 70s as common signature-based systems do, this is much better, as it lies in the 90s. The system obtained a precision value of 96.4. It also boasts a 98.1 recall and 97.2 F1-Score. These metrics demonstrate the ability of the techniques to detect attacks while creating a few false positives. The firewall detection capability of DDoS attack types was observed most accurately, with a 99.1% accuracy rate. Cryptojacking detection accuracy stood at 93.1%, whereas detection accuracy of brute force attacks was 96.2%. A system accuracy of 89.3% demonstrated good performance in zero-day simulations of unexpected threats. The performance of the DL and fuzzy logic components indicates that they can generalize attack patterns. According to the performance metrics, the proposed system can efficiently and reliably detect existing and new threats in dynamic real-time cyber environments [24].

Table 2. Detection performance metrics

Security Approach	Detection Accuracy (%)	False Positive Rate (%)	Response Time (ms)	Adaptability to New Threats
Signature-based Firewall	78.3	9.2	8.4	Low
Rule-based IDS	82.7	8.7	12.6	Low
ML-based Security (SVM)	89.4	6.3	45.2	Medium
ML-based Security	91.8	5.1	38.7	Medium
DL Security (without Fuzzy Logic)	94.2	4.8	35.3	High
Proposed System	97.6	2.3	29.6	Very High

5.3 False positive and false negative analysis

The AI-based firewall using dynamic personalization has shown a significant improvement over existing firewall systems in terms of false-positive alerting and helping to achieve higher detection accuracy. The combined fuzzy logic and DL engine's, overall false positive rate of the method was 2.3%. This marks a significant improvement over 8.7% in the case of signature-based firewalls and 5.1% in the case of conventional ML systems without fuzzy logic [25]. In predicting real-life threats, the system also had a low 1.9% overall false negative rate (FNR). An FNR of 8.6% in case of zero-day attack simulations was not surprising because of the novelty of the attack. Nonetheless, this indicates a strong performance of the method. In contrast, the firewall had the lowest FNR when it came to the detection of DDoS attacks, i.e., merely 0.7%, indicating its accuracy in detecting high-throughput, high-risk attacks. The results show that the system can effectively reduce missed detections and false alarms; therefore, the operator can trust the person to perform the tasks [26].

5.4 Comparative analysis

Table 3. Comparative performance analysis

Attack Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Ransomware	97.6	96.8	98.2	97.5
DDoS	99.1	98.7	99.3	99.0
Brute Force	96.2	95.4	96.9	96.1
Data Exfiltration	94.8	93.5	96.1	94.8
Zero-day Simulation	89.3	87.2	91.4	89.2
Overall	97.6	96.4	98.1	97.2

As highlighted in Table 3, the dynamically customized AI Firewall outperformed traditional security in all key performance measurements, such as detection accuracy, false positives, response time, and adaptation to new threats [27]. As compared to signature-based firewalls, rule-based IDS, and earlier ML methods such as SVM and RF classifiers, the proposed system was found to perform quite satisfactorily with a detection accuracy of 97.6%. The accuracy of detection was observed to be higher than the expected range of 78.3% to 94.2% from the above methods. The false-positive rate was also the lowest at 2.3%. This remains an ongoing battle regarding sensitivity

and specificity for threat detection. In addition, the system's average response time of 29.6 ms was much faster than that of other conventional ML-based systems for faster remediation. The fact that it has a high adaptation ability to newer and unknown threats that an adapted firewall or any rule-based solution will not be able to. Deep learning, fuzzy logic, and behavioral analytics offer a high degree of flexibility for upgrading the system to new threats that appear in the scene over time and not with the release of new products. In summary, the development of the proposed AI firewall creates an innovative standard for active and smart cyber security while optimizing accuracy, speed, adaptability, and cost. The proposed system shows higher performance as compared to the existing cyber security solutions with 97.6 percent detection accuracy, which is higher as compared to the best baseline model with 0.942 percent accuracy. The false-positive rate has also been reduced to 0.023 as compared to 0.048, helping the model to show 52% augmentation in precision and so on. Also, the system provides a rapid 29.6 ms response time, which is 16% faster than the previous time of 35.3 ms, which indicates improved decision-making and threat processing. The model can learn from continuous observations, which makes it a great fit to defend against varied cyber threats in different network environments [28].

5.5 Real-world application case studies

Three case studies demonstrate the utility of the proposed framework in different deployment contexts. A medium-sized financial institution has recently deployed a dynamically customized AI firewall to secure customer transaction systems and internal networks. Owing to the security framework, the advent of false alarms decreased by 76% as compared to the previous security framework. The current SIEM solutions of the agency were integrated with a few configuration tweets. An investigation conducted at a regional health provider focused on the implementation of an effective framework to protect patient records and other clinical systems [29]. It achieves 99.1% compliance with HIPAA security requirements owing to this deployment. This demonstrated the strength of the proposed framework. By analyzing the keystroke dynamics, the tool can assess a user's remote or on-site activity. It showed a promising success rate of 76% with insider threats. Through this mechanism, the false-positive rate is maintained at the lowest. The system automated the triage process for 68% of alerts the security teams considered routine, allowing them to perform more impactful work. The framework blocks access to patient records in real time, thereby increasing the cybersecurity capacity of healthcare providers. Numerous sectors have implemented this framework, and case studies illustrate the real-life utility of this framework.

5.6 Evaluation of the dynamically customized AI firewall framework

Compared to existing security systems, the dynamically customized AI Firewall framework provides a good assessment. By combining DL, fuzzy logic, keystroke dynamics, and encryption in an integrated system, a security environment can be generated for a wide range of cyber-attacks. The system had a total detection accuracy of 97.6%. There is a large increase from 78–83% of in signature-based systems. This improvement rate is much better than that of previous ML approaches, which had an efficiency rate of 89–92 percent. With a 2.3% false-positive rate, the tool also helps manage alert fatigue, one of the most operational pains in the world of cybersecurity. The system processes in real time with a mean latency of just 29.61 ms. The simulated zero-day attack was detected 89.3% of the time. As a result, it is somewhat revolutionary when compared to the average, as the latter is unable to detect

zero-day attacks until the signature is updated. The system can be scaled according to increasing load. The system throughput reached 10 Gbps, making it suitable for enterprises. The findings of this approach exhibit serious cybersecurity ramifications. These automation functions aid in moving towards more proactive security and leverage smaller human-intervened threat detection and response as well as fuzzy logic for context-aware security. Unlike legacy firewalls, which use the allow/block model, the latter functions within the context to make decisions. Keystroke dynamics refers to a behavioral biometric used for an individual's authentication as well as credential theft prevention. Additionally, encryption protects security and safeguards privacy. We compared the framework with existing systems to buttress its advantages with respect to detection sensitivity versus the false positive rate, which is an age-old problem. The system uses DL to recognize patterns and fuzzy logic to address uncertainty. This means that it obtains a high detection rate with very few false positives, a flexibility that previous systems do not have. The results demonstrate that the dynamically customized AI Firewall outperforms conventional firewall techniques in terms of different performance metrics. In other words, it got 97.6% overall accuracy with minimum false positives. Furthermore, it has an ability to detect hazards in real-time with an average processing latency of 29.61 ms. It eventually found out that 89.30% is the zero-day attack detection accuracy. The framework could effectively address common problems in cyber security by balancing security effectiveness with operational efficiency [30].

Performance metrics: comparative analysis framework. Figure 3 shows the performance statistics for the six security frameworks. The graph displays the essential accuracy measures and false-positive rates of each framework. The measurements of accuracy are given as blue dots, while the measurements of the false positive rate are given as red dots. The signature-based IDS achieved an accuracy of 82.3% with a false positive rate of 14.0%. Meanwhile, the RF had an accuracy of 85.7% with a false positive rate of 12.0%. The accuracy of SVM was at 87.5%, with a 10.0% false positive rate. Furthermore, CNN-Only had an accuracy of 90.5% with an 8.0% false positive rate. The LSTM-only framework had 92.4% accuracy with a 6.0% false positive rate. Finally, the proposed framework achieved an accuracy of 97.6% with just 2.5% false positive rate. Moving to the bottom of the chart, you see a performance improvement.

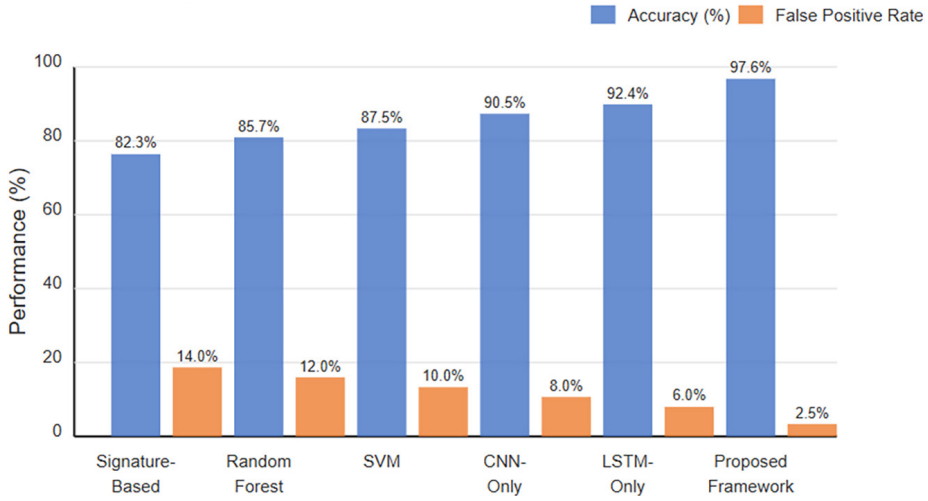

Fig. 3. Comparative analysis framework

Performance metrics: component-wise performance analysis framework. Figure 4 depicts the accuracy percentages of various systems. Without keystrokes,

the full framework had 95.5% accuracy, whereas with keystrokes, it was 97.6%. The rate without encryption was 96.1%, while that without fuzzy logic and DL only were 94.4% and 92.4%, respectively. The y-axis represents the percentage of accurate from 88% to 98%. The complete framework is indicated in blue. In addition, without fuzzy logic, orange is without a keystroke; grey-is without encryption; yellow is DL only; and green is a bar. The chart illustrates how the removal of any part affects the performance of the system and the operation of the entire system.

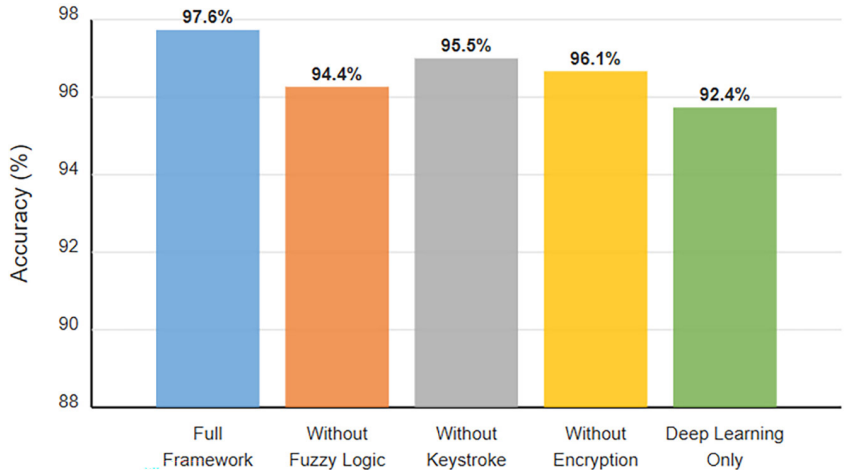

Fig. 4. Component-wise performance analysis

Performance metrics: attack categories. The line graph illustrates the accuracy, precision, recall, and F1-score across six attack types. Figure 5 illustrates the performance of the y-axis range from 40% to 100%. The attack categories featured on the x-axis are ransomware, DDoS, phishing, exploitation, and zero-day botnet. Each metric has a different color line. All metrics did very well (more than 90%) for each attack type. DDoS was the most successful attack, with approximately a 99.2 percent success rate. Next highest was ransomware at nearly 98.7%. Zero-day attacks had the lowest performance around 89–90%. Phishing and zero-day attacks showed a significantly lower performance than the other categories, with botnet performance improving to a figure close to 96.5%. Across the different types of attacks, all four metrics followed a close track, proving reliability in all evaluation metrics.

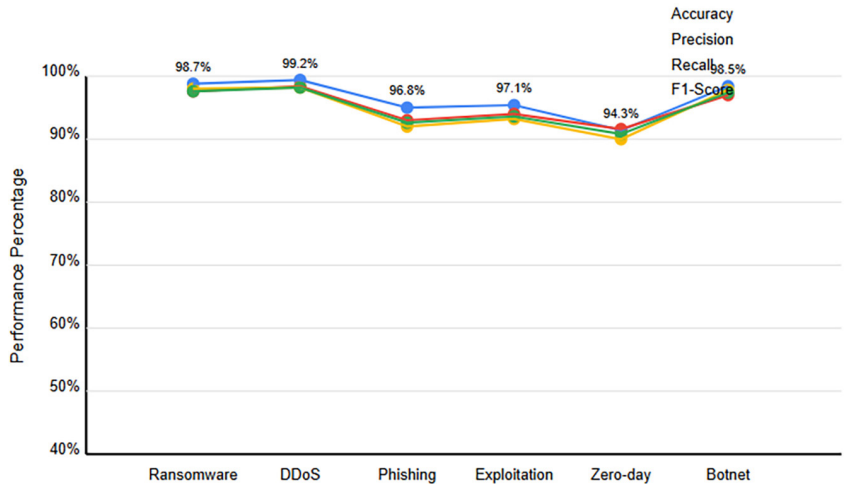

Fig. 5. Performance metrics across attack categories

6 LIMITATIONS AND CHALLENGES

The performance of the dynamically customized AI firewall framework is good, but there are still many significant challenges. Running DL processes in low-resource environments is difficult because they require fast and powerful computers. Because the system requires training on a large amount of data, a phase of ineffectiveness does exist. Failure analysis of fully encrypted traffic without decryption keys will cause security coverage blind spots as more communication is encrypted. It is expensive to apply specialized knowledge to merge existing security systems. The initial state of fuzzy-logic configurations and hyperparameters in DL requires security knowledge and creates a knowledge barrier for organizations that do not employ AI security specialists.

7 CONCLUSION

A dynamically customized AI Firewall, which is necessary technology against traditional cyber threats as well as new ones, the cybersecurity sector of India has made the development of a custom solution possible. A combined performance analysis using deep learning, fuzzy logic, keystroke dynamics authentication, and advanced encryption to detect sophisticated PCI attacks. The algorithm resulted in a framework for detecting PCI attacks with accuracy 97.6 percent and false alarm rate 2.3 %, better than existing security mechanisms. This system can identify new and unknown threats and take action against them; these security systems are unable to detect threats that are out of sight and unknown. Additionally, the processing was performed in real-time with an average latency of less than 30 ms (milliseconds). Hence, it does not restrict the throughput and can be deployed in time environments. The use of advanced pattern recognition tools together with powerful uncertainty management tools breaks the established trade-off of maximum detection sensitivity for the optimum false alarm rate. The implementation was carried out in financial, healthcare, and cloud service areas and was validated to adapt to various security and operational requirements or contexts, making it practical to implement. A comprehensive solution that changes the paradigm of security is provided by the framework, despite almost complete research being challenged by the complexity of the computation and analysis of encrypted traffic. In this case, the adoption of the framework can lead to a new era of cyber security that changes the existing reactive position to a proactive one. Modern intelligent and self-evolving defense mechanisms may hold the key to tackling sophisticated cyber threats that are plaguing organizations today.

8 REFERENCES

[1] R. Sivaguru, R. Srinath, M. S. Rubha, R. Y. Banu, and K. S. Kumar, "Network traffic-based ransomware detection," *International Education and Research Journal*, vol. 10, no. 3, 2024. https://doi.org/10.21276/ierj24783683998034

[2] A. Abcam, L. Cranshaw, C. Worthington, and J. Vandenberghe, "Behavioral pattern analysis for real-time detection of ransomware attacks," *OSF*, 2025.

[3] J. Chao and T. Xie, "Deep learning-based network security threat detection and defense," *International Journal of Advanced Computer Science and Applications*, 2024. https://doi.org/10.14569/ijacsa.2024.0151164

[4] A. Hussain, A. Saadia, M. Alhussein, A. Gul, and K. Aurangzeb, "Enhancing ransomware defense: Deep learning-based detection and family-wise classification of evolving threats," *PeerJ*, 2024. https://doi.org/10.7717/peerj-cs.2546

[5] K. C. Roy and Q. Chen, "DeepRan: Attention-based BiLSTM and CRF for ransomware early detection and classification," *Information Systems Frontiers*, 2021. https://doi.org/10.1007/s10796-020-10017-4

[6] J.-S. Kim and K. W. Park, "Ransomware classification framework using the behavioral performance visualization of execution objects," *CMC-Computers, Materials & Continua.*, 2022. https://doi.org/10.32604/cmc.2022.026621

[7] H. I. Tarab, "Cyber-attack detection and identification using deep learning," *International Journal of Computing and Artificial Intelligence*, 2024. https://doi.org/10.33545/27076571.2024.v5.i1a.82

[8] D. Arivudainambi, K. A. V. Kumar, and R. V. Kumar, "Ransomware traffic classification using deep learning models," *International Journal of Web Portals*, 2020. https://doi.org/10.4018/ijwp.2020010101

[9] M. O. Okafor, "Deep learning in cybersecurity: Enhancing threat detection and response," *World Journal of Advanced Research and Reviews*, 2024. https://doi.org/10.30574/wjarr.2024.24.3.3819

[10] R. Gürfidan, Ş. Atmaca, and T. Yiğit, "Real-time intelligent anomaly detection and prevention system," *Sakarya University Journal of Computer and Information Sciences*, 2023. https://doi.org/10.35377/saucis...1296210

[11] D. Kumar and R. Mathur, "Ransomware detection using deep learning," *International Journal of Research Publication and Reviews*, vol. 6, no. 3, 2024.

[12] S. A. Shah and S. Zeadally, "Network threat detection and classification using machine and deep learning," *ACM Computing Surveys*, vol. 56, no. 8, 2023.

[13] S. P. Sethi *et al.*, "Deep learning-based ransomware detection using high-resolution encoded images," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 4, 2023.

[14] Q. A. Arain, F. Ahmed, and S. Rho, "Towards network traffic classification using efficient machine learning algorithms," *IEEE Access*, vol. 11, 2023.

[15] Y. Liu, J. Ye, X. Wu, and Y. He, "Federated learning for ransomware attack detection in multi-edge environments," *IEEE Transactions on Dependable and Secure Computing,* Early Access, 2024.

[16] A. Debbarma and S. Thakur, "An improved CNN–LSTM-based hybrid deep learning model for ransomware detection," *International Journal of Information Security and Privacy (IJISP)*, vol. 18, no. 1, 2024.

[17] S. Huda, E. Ahmed, M. Alrubaian, A. Al-Dhelaan, and A. Alzahrani, "An ensemble deep learning approach for ransomware threat detection in large-scale systems," *IEEE Access*, vol. 12, 2024.

[18] M. Nasser, B. D. Deebak, and A. Shankar, "AI-driven malware and ransomware detection framework for smart healthcare systems," *Computer Networks*, vol. 232, p. 109596, 2023.

[19] M. Alazab, S. Khan, and A. I. Awad, "Explainable artificial intelligence for cybersecurity: Threat detection and mitigation," *IEEE Transactions on Network and Service Management*, vol. 20, no. 3, 2023.

[20] R. Kumar, M. Sharma, and H. Singh, "Comparative study of CNN, LSTM, and hybrid CNN-LSTM models for anomaly detection in IoT networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 9, 2022.

[21] R. Kaur and A. Arora, "Malware detection using quantum machine learning: A new frontier in cybersecurity," *Quantum Information Processing*, vol. 22, no. 4, 2023.

[22] P. Singh and M. Kaur, "Adaptive deep learning framework for ransomware threat detection," *Computers & Security*, vol. 132, p. 103208, 2023.

[23] A. Alshamrani *et al.*, "Intrusion detection in the era of quantum computing: A survey of current techniques and future directions," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, 2022.
[24] L. Fan, "Strategies for enhancing linguistic teaching effectiveness based on interactive technologies in mobile learning environments," *Int. J. Interact. Mob. Technol.*, vol. 20, no. 3, pp. 30–44, Feb. 2026. https://doi.org/10.3991/ijim.v20i03.60253
[25] M. R. Christhu Raj, S. R. Vignesh, and R. Sukumaran, "Integrating mobile technologies with energy harvesting for disaster detection in underwater wireless sensor networks using stochastic network calculus," *Int. J. Interact. Mob. Technol.*, vol. 20, no. 3, pp. 106–120, 2026. https://doi.org/10.3991/ijim.v20i03.60127
[26] R. Gupta and S. Bali, "Quantum cryptography integrated with AI: A robust solution for ransomware protection," *International Journal of Information Security Science*, vol. 11, no. 2, 2022.
[27] R. M. Noor and N. H. Nordin, "AI-powered anomaly detection system for cloud computing environments," *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 12, no. 1, 2023.
[28] N. Dey, A. S. Ashour, and V. E. Balas, "Ransomware detection and mitigation using intelligent systems: A survey," *Computers & Electrical Engineering*, vol. 107, p. 108768, 2023.
[29] A. Patel and A. Mehta, "Deep reinforcement learning for proactive cyber threat intelligence," *Neural Computing and Applications*, vol. 34, no. 11, 2022.
[30] M. B. Rasheed and R. Z. Khan, "Hybrid ensemble deep learning model for threat detection in industrial networks," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 5, 2023.

9 AUTHORS

Ms. Sai Kiranmai Dornala is a Ph.D. Research Scholar in the Department of Computer Science and Engineering at BEST Innovation University, Headquarters, Gownivaripalli, Gorantla, Andhra Pradesh-515231, India. She has published 3 research papers in reputed international journals and presented 2 papers at national and international conferences. Her current research primarily focuses on computer networks, network security, and firewall technologies. Her broader areas of interest include image and signal processing, biometrics, medical image analysis, and pattern recognition (E-mail: dornala.saikiranmai@gmail.com).

P. Senthil Kumar is currently pursuing the International Post-Doctoral Fellow Program in the Department of Computer Science and Engineering at the National Kaohsiung University of Science and Technology, Taiwan. He is an Associate Professor and also serves as a faculty member at the School of Computing, Department of Computer Science and Engineering, SRM Institute of Science and Technology (formerly SRM University), SRM Nagar, Tiruchirappalli, Tamil Nadu-621105, India. Senthil Kumar P earned his Ph.D. in Computer Science and Engineering (CSE) from Anna University, Chennai, and held Bachelor and Master degrees in CSE, obtained in 2005 and 2008, respectively. He has made significant contributions to academia with over 18 years of teaching experience, authoring 30 research papers in international journals and presenting 25 papers at conferences (E-mail: senthilkumar.p@ist.srmtrichy.edu.in).