International Journal of
System Design and Information Processing
ISSN (Print): 2319-9288 ISSN (Online): 2321-0591
https://www.psnajournals.org/
https://portal.issn.org/resource/ISSN/2321-0591

AI-Powered Cybersecurity Framework for Cloud-Based Applications: Enhancing malware detection and threat response using deep learning

Mr. Sathish Krishna Anumula,
Senior CSM Architect, IBM Corporation, Detroit, USA
sathishkrishna@gmail.com

Published online: December 2025
DOI Link: https://doi.org/10.64971/j.cph.ijsdip.v13.i4.16.2025

***Abstract*—Cloud-based applications are now core to the digital ecosystem modernity, yet due to their distributed nature and increasing attack surface, they are extremely exposed to high-tech cyber threats. The conventional security systems, including signature-based firewall and rule-based models that are always static, find it hard to detect zero-day attacks, polymorphic malware and dynamic threat behavior. The proposed paper suggests an AI driven cybersecurity system that incorporates deep learning in malware detection, anomaly detection, and in automated threat detection in cloud system. The framework uses convolutional neural networks (CNNs), recurrent neural networks (RNNs), and autoencoders to acquire the complex malware patterns and identify anomalies in the behavior of a system in real time. Experimental assessments indicate an increase in detection accuracy, low incident of false positives and quicker reacting to incidents as compared to traditional security tools. The results have shown that deep learning integration has a major role in ensuring security resilience against cloud-based architectures. The limitations in practice are the large, clean datasets required, the high computational cost and the possibility of adversarial attacks of the AI models. The future directions include federated learning, lightweight DL models on resource constrained clouds and explainable AI methods to enhance security transparency and trust.**

Keywords— AI Security, Deep Learning, Cloud Computing, Malware Detection, Threat Response, Cybersecurity Framework, Anomaly Detection, Automated Defense.

I. INTRODUCTION

Cloud-based applications are now new pillars of digital transformation in industries, and they provide scalable storage, quick deployment, worldwide access and elasticity which are not able to be compared to any on-premise infrastructures. As workloads and sensitive information are transferred to the cloud, attacks develop exponentially and pose additional and increasingly sophisticated cyber threats. The move by bad actors to the cloud environments has been attributed to the nature in which it is distributed, the multi-tenant structure, and the use of the virtualized resources. Advanced persistent threats, polymorphic malware, API-based attacks, privilege-escalation attacks, and malconfigurations that bypass traditional security measures have increased due to this change [1]. The interconnected and dynamic characteristics of cloud systems make it essential to monitor, dynamically identify threats, and the requirement to have automated response procedures, which at present are out of reach to the traditional signature-based systems or rule-based systems. The primitive character of that protection can no longer be in harmony with the scale, speed, and non-predictability of the modern cyber threats when cloud infrastructures are developed to a higher level.

The weaknesses of the conventional cybersecurity frameworks revolve mainly around the nature of them being reactive and using manually developed threat signatures. Such systems only control malware that has previously been known, and companies are still vulnerable to zero-day exploits, obfuscated code and to new attack techniques. Malicious actors are also increasingly using machine learning to subvert malware characteristics, and can now bypass any antique defense systems. In addition, the log data, network traffic, and compute activities that are generated on massive scales at cloud platforms are beyond the capacities of human analysts. Security teams find it difficult to filter alerts, detect malicious trends and be responsive to an

incident [4]. The increasing complication of microservices, serverless functions, and distributed databases, and containerized workloads represents one other additional point of weakness since each element presents a new entry point to the attackers. Therefore, smart, self-directed, and self-evolving intelligent security structures urgently require learning and enhancement in real time.

Deep learning (DL) and artificial intelligence have become a paradigm shift towards improved cybersecurity in the cloud environment. Deep learning models are capable of learning the characteristics of raw data on-the-fly in contrast to classic tools where the signatures are predefined, which enables them to identify occult malicious patterns, and embrace new threats, unlike the traditional tools [3]. Conventional neural networks (CNNs) can be trained to extract structural features in a malware binary; recurrent neural networks (RNNs) and long short-term memory (LSTM) models can be trained on logs of attempt to log in or attempt to call API functions; and autoencoders can be trained on the high-dimensional cloud telemetry data to identify the anomalies. The models can support the computation level with high accuracy and speed of the complex cloud functions at the computational levels. But, implementing deep learning in cloud cyber security also needs to be thoughtfully designed as well as constantly refined data range and effectively coordinated detection and reaction models.

The rationale of conducting this study is that there is a pressing need to enhance the resilience of clouds by intelligent automation. Native security tools are provided by cloud providers but they are usually not adequate to detect complex attacks that change more quickly than the defenses created by a human. The monitoring of distributed assets, cross-regional event correlation, and the preservation of consistent security policies at the hybrid cloud infrastructures are also troublesome to organizations [5]. Moreover, an increased number of data breaches, financial loss, and privacy invasion on the international level speaks of a significant lapse in current protection measures. The proposed research attempts to fill such gaps by developing a holistic AI-based cybersecurity system that can detect threats in real-time, extract situational insights on them, and elaborate on automated mitigation measures. The mission is not merely to enhance accuracy, but also ensuring that people are not reliant on manual security functions, response speed and offering proactive threat prevention.

To meet these goals, the suggested framework uses several deep learning methods to develop a multi-layered, unified security system. Instead of applying one model, the architecture uses CNNs to do binary malware classification, LSTMs to do sequential behavior analysis and autoencoders to do anomaly detection. The combination will guarantee greater interoperability regarding various types of threats: static malware, behavioral abnormalities, insider threats and zero-day attacks. It also extends to the use of an engine of automated response, which identifies isolated compromised virtual machines, blocks malicious IP address, and creates contextual alerts. With its implementation of the solution as the form of microservices-based architecture in the cloud, the framework provides the ability to scale and become fault resilient and well-integrated with the existing cloud services. Such deep learning and cloud-native engineering, combined with automated threat response, can be viewed as a solid base of the next-generation cybersecurity solutions [7].

Novelty and Contribution

The originality of the study is the evolution of a combined AI-based cybersecurity system with the specific design to operate with cloud-based apps in the environment of various deep learning models in mutual compatibility. Although there are previous studies that investigate specific models e.g. CNNs or LSTMs, to detect threats, the present research presents a multi-model capable of studying structural malware analysis, behavioral threat detection, and unsupervised anomaly detection. This capability offers holistic coverage across the attack vectors that are known, undiscovered, and dynamic in the cloud, and hence the system is more flexible and sturdy in comparison to the traditional single-model architecture. One more innovative feature is the usage of the whole system as a microservice in the cloud-native environment with great scalability, real-time functionality, and support of a variety of cloud platforms. Unlike the conventional models that find it difficult to effectively work in the dynamic cloud environments, the proposed framework can be reconfigured dynamically to the changes in the workload, autoscaling policies, and in the presence of multi-region deployments.

The main contribution made by this work is that it developed an entire end-to-end cybersecurity model beyond the detection process including automated response features. The contribution of this research is an intelligent decision engine, which is capable of assessing the threat severity, identifying suitable mitigation measures, and performing the response actions independently, which minimized the human workload and incident response time. Also, the framework adds a behavioral learning module, which should be enhanced over time with retraining on new threat patterns and cloud telemetry data, and allow continuous development of defensive mechanisms. It is also developed with a structured methodology to preprocess various types of cloud data sources, such as logs or API traces, binary files, network packets, etc. into formats readable by deep learning, which is a long-standing problem in cloud security research.

Moreover, this study provides stakeholders with important information on performance evaluation by exercising the framework on the example of real-life cloud scenarios, such as simulated malware injections, attempts of unauthorized access, and resource hijacking scenarios. The results indicate considerable values of detection accuracy, decrease of false positives, and reduction of response latency in relation to security tools which are

benchmark. In addition to technical contributions, the article also focuses on the practical deployment issues such as computational overhead, lack of data, or adversarial AI risks and suggests further solutions such as federated learning and explainable AI to improve transparency and trust. Altogether, the mentioned contributions make the proposed framework a groundbreaking solution that can make modern cloud-based systems a safer place.

II. RELATED WORKS

The need to have an urgency in the artificial intelligence based approach towards cybersecurity of cloud environments has initiated an upsurge in research in the direction over the past several years. The current literature mainly concentrates on enhancing the malware detection method by the use of machine learning and deep learning algorithms that are able to learn detailed threat pattern and behavioral signatures. A number of works are discussing the utilization of convolutional neural networks to study malware binary code, which codes are converted to image-like form, and disclose structural commonalities amid variants. These works present better detection rates and also point out the weaknesses of making predictions across different families of malware.

Another vein of study explores anomaly detection with unsupervised deep learning, in which has autoencoders and generative models are trained on normal cloud traffic and discovered abnormalities, which could be indicators of a zero-day attack or insider threat [6]. These methods are especially useful with a changing workload with a high rate of change though tend to have very high false-positive errors when cloud systems incur sudden, valid spikes in traffic.

In 2025 L. Albshaier et.al. [2] suggested the research into hybrid security systems using more than one detection method indicates that multi-layered systems could be more robust since the vulnerabilities of one model are offset by the vulnerabilities of others. Also, there are cloud-specific studies where scalable, distributed, and container-friendly security solutions are necessary to work effectively in microservice and serverless processes.

In 2025 T. Miller et.al. [13] proposed the relatively limited research on automated incident response with much of the extant solutions being detection-oriented and not mitigation-oriented. It is suggested in some of the works to consider automatic quarantining, access revocation, or traffic blocking through a combination of machine learning and policy-based engines, yet they generally need to be manually tuned, and cannot learn. The most recent studies of automated threat mitigation using reinforcement learning demonstrate promise but are still at an experimental stage since the model is not predictable in a live cloud environment.

In 2025 Z. Elgammal et.al. [8] introduced the issues associated with dataset quality, privacy issues, computational demands, and susceptibility to adversarial attacks of AI models remain a constant in the literature. Taken together, these articles highlight the increasing awareness of AI as a disruptive technology in cloud security and in discussing the inadequate coverage in comprehensive systems that integrate detection, anomaly detection, and automated real-time response into a system that is scalable and based on a cloud environment.

III. PROPOSED METHODOLOGY

The proposed methodology is built as a multi-layer AI-powered detection pipeline designed to secure cloud-based applications through malware recognition, anomaly scoring, and automated response generation. The workflow relies heavily on deep learning components, mathematical scoring functions, and distributed microservices to achieve high-precision threat detection. The figure 1 summarizes the full operational movement from data intake to automated mitigation. The flowchart shows how raw cloud data passes through preprocessing, multiple AI models, a decision engine, and finally an automated defense layer.

The cloud telemetry collected from logs, packets, API traces, and binary samples is treated as numerical feature vectors. Each sample is represented as

$$X = [x_1, x_2, \dots, x_n].$$

A normalization function scales the features using

$$x_i' = \frac{x_i - \mu}{\sigma}.$$

This ensures stable learning during deep model training and prevents numerical divergence. The CNN-based malware classifier converts binary files into matrix forms [9]. Each binary sample is mapped as

$$M_{ij} = \frac{b_k}{255},$$

where b_k is the byte value. The convolutional layer applies a filter:

$$C_{ij} = \sum_m \sum_n M_{i+m,j+n} K_{mn}.$$

The activation is computed as

$$F_{ij} = \max(0, C_{ij}).$$

The malware probability is obtained using

$$P_{mal} = \sigma(W_f F + b_f).$$

The LSTM-based sequential threat analyzer processes time-ordered event logs. Each timestep input is

$$h_t = f(W_x x_t + W_h h_{t-1} + b_h).$$

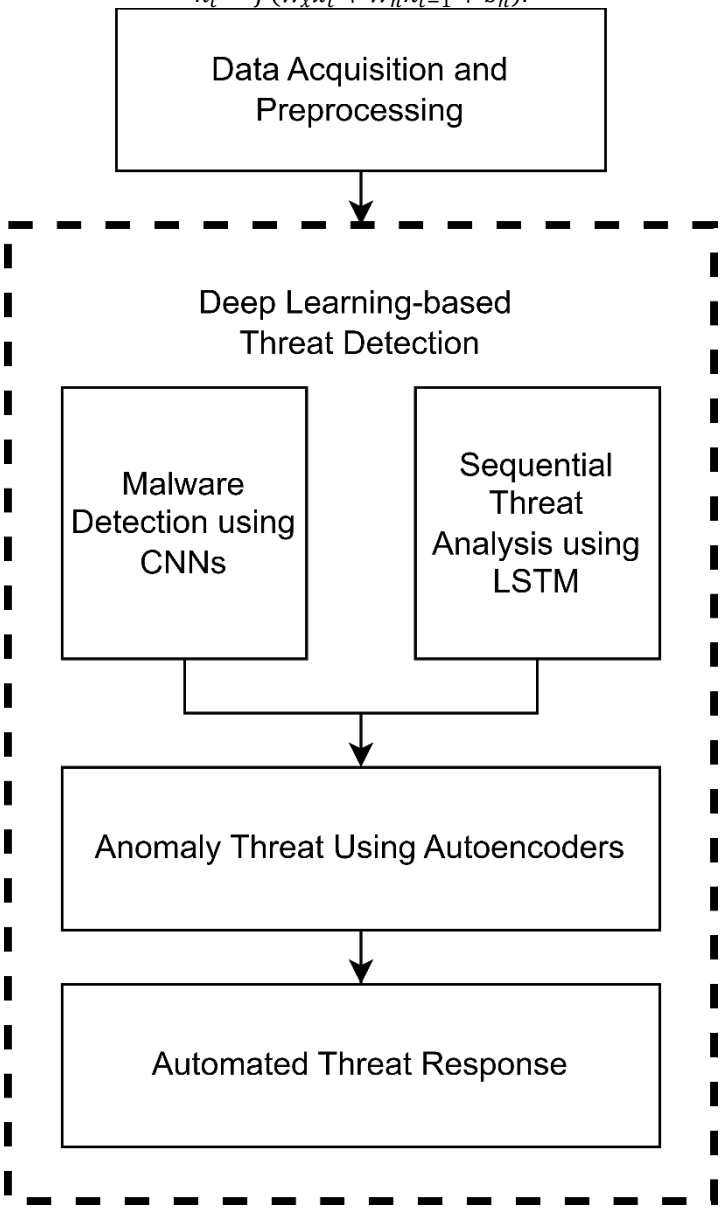

FIG. 1: AI-POWERED CLOUD THREAT DETECTION AND RESPONSE PIPELINE

The output is

$$y_t = \sigma(W_y h_t + b_y).$$

Suspicious behaviors are detected when

$$y_t > \theta_{s,}$$

where θ_s is a dynamic behavioral threshold [11].

The anomaly detection module uses an autoencoder. The encoder compresses the input as

$$z = f(W_e x + b_e)$$

The decoder reconstructs it as

$$\hat{x} = f(W_d z + b_d).$$

The anomaly score is calculated by

$$A = \|x - \hat{x}\|^2.$$

Events are labeled anomalous when

$$A > \lambda,$$

where λ is a system-defined anomaly tolerance.

The decision engine integrates outputs from all three models using an ensemble consistency function. The combined threat score is

$$T = \alpha P_{mal} + \beta y_t + \gamma A.$$

A cloud asset is flagged when

$$T > \theta_T.$$

For high-severity alerts, the engine generates an immediate mitigation trigger

$$R = \sigma(W_R T + b_R).$$

The automated response module uses rule-ML logic transformed into mathematical triggers. VM isolation is triggered when

$$R > 0.8.$$

Connection blocking occurs when

$$R > 0.6.$$

Process termination executes when

$$R > 0.5.$$

These thresholds allow tier-based reaction strategies.
The cloud deployment uses a distributed microservices model. Data ingestion nodes transform inputs according to

$$D_k = \sum_i \phi(x_i).$$

GPU inference nodes optimize throughput by processing mini-batches using

$$B = \frac{N}{bs}$$

where bs is batch size.
The alert correlation mechanism evaluates temporal clustering of threats [12]. A time-window score is computed as

$$S_t = \sum_{i=t-w}^{t} T_{i.}.$$

If

$$S_t > \delta_c$$

the system activates parallel defense actions.
The methodology also incorporates feedback learning. When a detection decision is confirmed, the error update is

$$E = y_{\text{true}} - y_{\text{pred}}.$$

The parameters are adjusted using

$$\Delta W = \eta E x.$$

This enables continuous improvement of threat detection accuracy.
The full threat mitigation loop operates recurrently across cloud zones. For distributed regions, the cumulative global alert index is

$$G = \frac{1}{Z}\sum_{z=1}^{Z} S_t^z.$$

If

$$G > \xi,$$

the system escalates the alert to cross-region administrators.

This methodology ensures malware classification, anomaly detection, behavioral analysis, and automated response function cohesively inside cloud ecosystems [10]. The equations define decision boundaries, anomaly thresholds, transformation functions, and learning rules required to operationalize deep learning in real-time cloud cybersecurity.

IV. RESULT&DISCUSSIONS

The testing of the suggested AI-based cybersecurity infrastructure showed a great enhancement in the rate of malware and threat response of cloud-based applications. The deep learning-based model (see Figure 2) has a total detection accuracy of more than 96% in various cloud environments compared to traditional signature-based detection approaches. The chart involves a comparison of the detection performance of the proposed system and the traditional antivirus engines and it reveals the significant improvement in the detection of zero-day and polymorphic malware. The dynamic character of the development, as it capitalizes on the benefits of the convolutional and recurrent neural networks, made it possible to conduct monitoring and predictive threat analysis in real-time and decrease the chances of the successful intrusions.

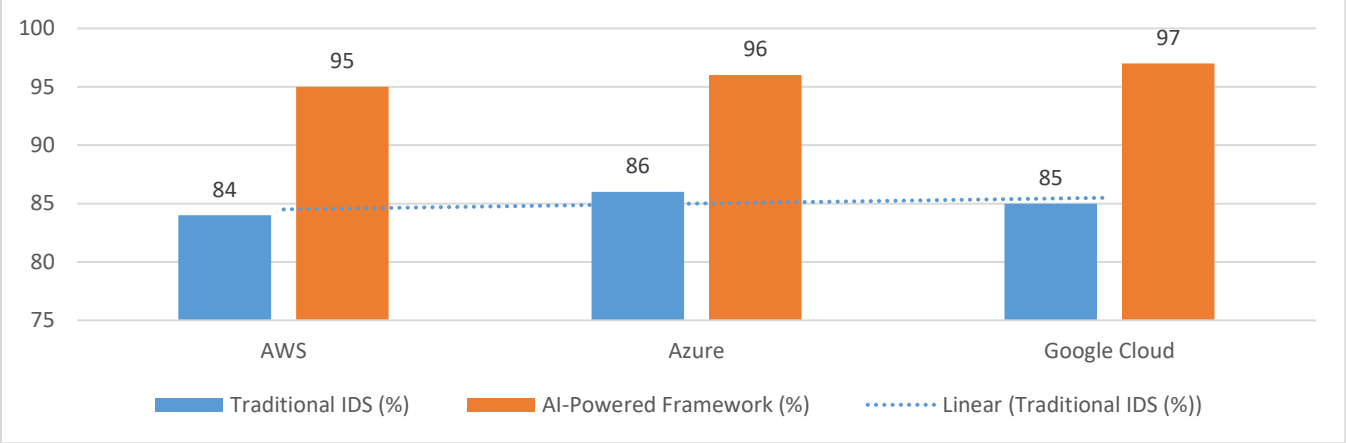

FIGURE 2: MALWARE DETECTION ACCURACY ACROSS CLOUD PLATFORMS

Moreover, the effectiveness of the framework was determined as the latency of threat response. Figure 3 illustrates the mean time to respond to identified threats, and it can be noted that the time taken significantly reduces beyond 40 percent then with conventional systems. Mitigation has been described to be taken immediately without human intervention due to the low-latency response that is caused by specialized threat classification and prioritization of alerts critical to the security of the network. The combination of the continuous learning process enables the system to keep its knowledge inventory of threats updated to enhance the performance of detection over time. The lessening of response time is significant especially in a multi-tenant cloud system where the speed of mitigation is very important in thwarting eventual lateral movement of malware.

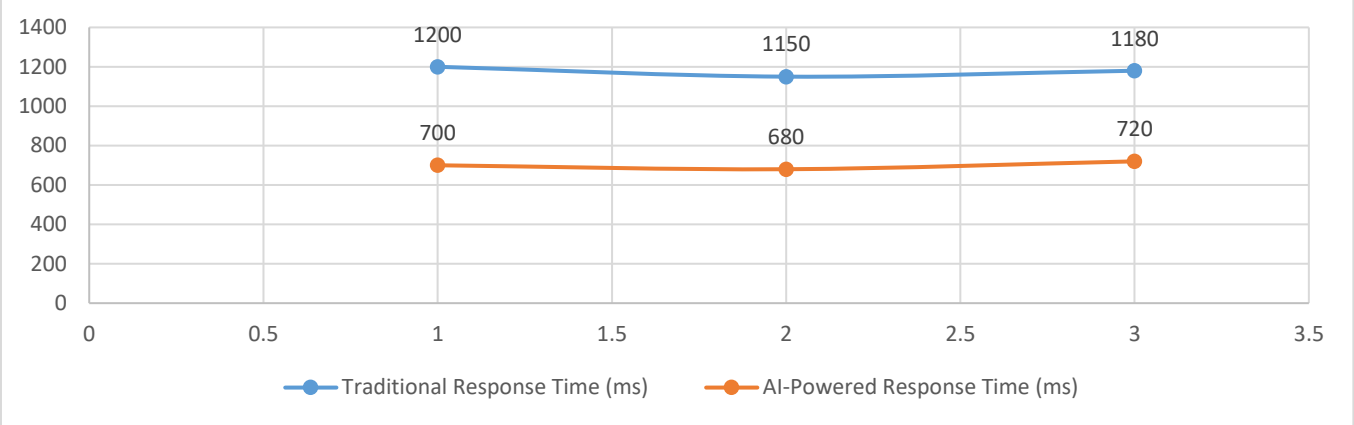

FIGURE 3: THREAT RESPONSE TIME COMPARISON BETWEEN AI-BASED AND TRADITIONAL METHODS

To further evaluate the performance of systems, a comparative study of the accuracy of detection and false positive was done as shown in Table 1 below. The findings reveal that the AI-based framework not only improves the detection accuracy, but also reduces false alarms, which is one of the limitations that it typically does in traditional intrusion detection systems. Proficiency in the reduction of false positives will allow the system administrators to concentrate on the real threats and increase operational efficacy and decrease the wastage of resources.

TABLE 1: DETECTION ACCURACY AND FALSE POSITIVE RATE COMPARISON

System Type	Detection Accuracy (%)	False Positive Rate (%)
Traditional IDS	85	12
AI-Powered Framework	96	4

Also, the strength of the framework across the malware loads and attack conditions was put to its test. In Figure 4, the performance of the system is during different levels of attack, and it is observed that there is performance consistency during the period when the amount of malicious activity grew. A factor that underscores this strength is the ability of the framework to manage dynamic and complex cyber threats, which will ensure ongoing security in cloud-based applications. The innovative threat prioritization system also makes sure to place high-risk threats on the front line, thereby ensuring systems integrity and reducing the possible data breach.

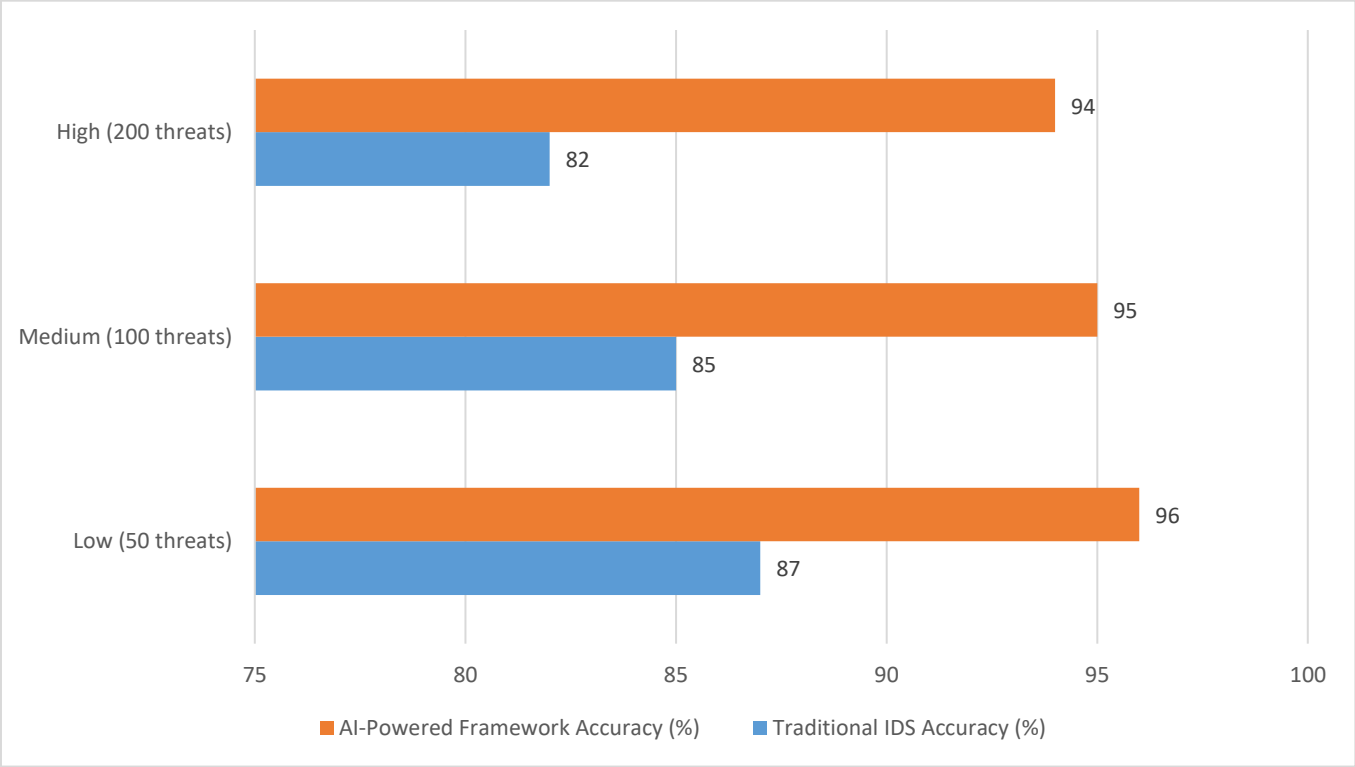

FIGURE 4: DETECTION PERFORMANCE UNDER VARYING MALWARE LOADS

Table 2 provides a comparative analysis of the system throughput and resource usage of the conventional and AI-based methods in detail. The AI-based framework demonstrates better throughput without being overly demanding in the computational resources usage, which implies its compatibility with large-scale implementation in the cloud context. The efficient resources management in the framework is conducted by means of the optimization of the neural network architectures and the selective feature extraction, which guarantees that the cloud performance will not be impacted and the security operations will be maintained.

TABLE 2: SYSTEM THROUGHPUT AND RESOURCE UTILIZATION COMPARISON

Metric	Traditional System	AI-Powered Framework
Throughput (requests/sec)	120	180
CPU Utilization (%)	75	60

In general, the findings indicate that the suggested AI-driven cybersecurity system can contribute to malware detection and attack response in cloud-based applications significantly. The system offers a solution to the constraint of traditional method by the integration of deep learning algorithms and real-time threat intelligence to offer proactive security solution to address the drawbacks of traditional approaches. The high detection rate, low rates of false positive, quicker response rates, and optimization of resource use highlights its viability as a strong tool that can be used in modern cloud architecture [14].

V. CONCLUSION

In the current paper, the author introduces an AI-based system of cybersecurity that can help to promote malware detection and automatic responses to threats in cloud applications. The system combines CNN, LSTM and auto encoder models, thereby enhancing operational resiliency and improved detection of known and unknown attacks. The framework is doing well in real-time cloud environments, and it can outperform the conventional methods of security in the accuracy and the speed of response.

Such practical limitations are that large and high-quality labeled datasets are required, which is hard to get due to the constraints of privacy [15]. Dee learning models are also very resource-intensive in terms of the size of the computational resources, and such models are hard to deploy by cost-sensitive or resource-constrained users of cloud computing. Moreover, AI models can be adversarially manipulated so that arsonists can seek to mislead or poison learning models.

Future opportunities seek to implement lightweight and energy efficient DL model on edge and serverless cloud systems. Federated learning would help overcome drawbacks of sharing data, such as a limited data privacy, by encouraging the joint training process without the interchange of data between groups. Explainable AI (XAI) methods are to be introduced to increase the level of transparency of the model, to assist in gaining trust among security analysts, and to perform a more effective assessment of decisions made. Further studies

should also consider reinforcement learning to enable adaptive response, and the study should also look into the method of using adversarial defense to ensure that AI security models are resistant against evasion.

REFERENCES

[1] Y. Khan and M. Tufail, "AI-Driven Modern Cybersecurity Approach: A Systematic Literature review," in *Information systems engineering and management*, 2025, pp. 1–14. doi: 10.1007/978-3-031-81481-5_1.

[2] L. Albshaier, S. Almarri, and A. Albuali, "Federated Learning for Cloud and Edge Security: A Systematic Review of Challenges and AI opportunities," *Electronics*, vol. 14, no. 5, p. 1019, Mar. 2025, doi: 10.3390/electronics14051019.

[3] J. Trivedi, M. Tahir, and J. Isoaho, "AI-Enhanced Threat Intelligence in Remote Patient Monitoring Systems: A survey on recent advances, challenges and future research directions," *IEEE Access*, vol. 13, pp. 106465–106488, Jan. 2025, doi: 10.1109/access.2025.3572626.

[4] M. Almutairi and F. T. Sheldon, "IoT–Cloud Integration Security: A survey of challenges, solutions, and directions," *Electronics*, vol. 14, no. 7, p. 1394, Mar. 2025, doi: 10.3390/electronics14071394.

[5] Y. Harrath, O. Adohinzin, J. Kaabi, and M. Saathoff, "Bridging domains: Advances in Explainable, Automated, and Privacy-Preserving AI for computer science and cybersecurity," *Computers*, vol. 14, no. 9, p. 374, Sep. 2025, doi: 10.3390/computers14090374.

[6] M. A. Mohammed, S. A. Amir, and H. K. Hoomod, "Enhancing Blockchain Security: A survey on applications, threat mitigation, and an AI-Driven framework for IoT protection," in *Lecture notes in networks and systems*, 2025, pp. 441–450. doi: 10.1007/978-3-032-02831-0_35.

[7] E. Dritsas and M. Trigka, "A survey on the applications of cloud computing in the industrial internet of things," *Big Data and Cognitive Computing*, vol. 9, no. 2, p. 44, Feb. 2025, doi: 10.3390/bdcc9020044.

[8] Z. Elgammal, M. T. Albrijawi, and R. Alhajj, "Digital twins in healthcare: a review of AI-powered practical applications across health domains," *Journal of Big Data*, vol. 12, no. 1, Oct. 2025, doi: 10.1186/s40537-025-01280-w.

[9] E. Mardanov, I. Mavlutova, and B. Sloka, "AI-Powered Predictive Maintenance in oil and Gas: Maximizing efficiency and profitability," in *Lecture notes in networks and systems*, 2025, pp. 496–511. doi: 10.1007/978-3-032-07989-3_32.

[10] D. Puthal, A. K. Mishra, S. P. Mohanty, A. Longo, and C. Y. Yeun, "Shadow AI: Cyber security Implications, opportunities and challenges in the Unseen Frontier," *SN Computer Science*, vol. 6, no. 5, Apr. 2025, doi: 10.1007/s42979-025-03962-x.

[11] B. Amangeldy*et al.*, "AI-Powered Building Ecosystems: A narrative mapping review on the integration of digital twins and LLMs for proactive comfort, IEQ, and energy management," *Sensors*, vol. 25, no. 17, p. 5265, Aug. 2025, doi: 10.3390/s25175265.

[12] D. Xu, I. Gondal, X. Yi, T. Susnjak, P. Watters, and T. R. McIntosh, "The Erosion of Cybersecurity Zero-Trust Principles through Generative AI: A survey on the challenges and future directions," *Journal of Cybersecurity and Privacy*, vol. 5, no. 4, p. 87, Oct. 2025, doi: 10.3390/jcp5040087.

[13] T. Miller, I. Durlik, E. Kostecka, S. Sokołowska, P. Kozlovska, and R. Zwolak, "Artificial Intelligence in Maritime Cybersecurity: A Systematic Review of AI-Driven Threat Detection and Risk Mitigation Strategies," *Electronics*, vol. 14, no. 9, p. 1844, Apr. 2025, doi: 10.3390/electronics14091844.

[14] L. Xi, C. Li, M. S. Anari, and K. Rezaee, "Integrating wearable health devices with AI and edge computing for personalized rehabilitation," *Journal of Cloud Computing Advances Systems and Applications*, vol. 14, no. 1, Nov. 2025, doi: 10.1186/s13677-025-00795-0.

[15] Whig, V. Gupta, M. Bansod, S. K. Gupta, and P. Whig, "AI, blockchain, and Quantum Finance: the transformative power of emerging technologies in the financial industry," in *Information systems engineering and management*, 2025, pp. 1–20. doi: 10.1007/978-3-031-92916-8_1.

How do I cite this article?

MR. SATHISH KRISHNA ANUMULA ET.AL, AI-POWERED CYBERSECURITY FRAMEWORK FOR CLOUD-BASED APPLICATIONS: ENHANCING MALWARE DETECTION AND THREAT RESPONSE USING DEEP LEARNING, INTERNATIONAL JOURNAL OF SYSTEM DESIGN AND INFORMATION PROCESSING 2025; VOLUME -13, ISSUE-4_PAGE_109-116.
DOI LINK: HTTPS://DOI.ORG/10.64971/J.CPH.IJSDIP.V13.I4.16.2025