Google Scholar Crossref doi scopus

Impact factor 6.2

Geoscience Journal

ISSN:1000-8527

Indexing:

- Scopus
- Google Scholar
- DOI, Zenodo
- Open Access

www.geoscience.ac

Registered

A Quantum Immune Temporal Bayesian Framework for Ultra High Accuracy AI Driven Intrusion Detection and Adaptive Mitigation in Elastic Cloud Computing Environments

Reteesh sharma P[1], Kumara babu V T[2], Harish Raghavender V[3], Tamilselvi P[4]

[1] Department of Computer Applications, Sathyabama Institute of Science and Technology, Chennai 600119, INDIA

[2] Department of Computer Applications, Sathyabama Institute of Science and Technology, Chennai 600119, INDIA

[3] Department of Computer Applications, Sathyabama Institute of Science and Technology, Chennai 600119, INDIA

[4] Department of Computer Applications, Sathyabama Institute of Science and Technology, Chennai 600119, INDIA

Abstract. Interactive resource implementation, multi-tenancy, and massive data transfer present an ever more complicated risk to cloud computing environments. Conventional intrusion detection systems are not effective in detecting new and sophisticated attacks within this environment. This paper attempts to solve this issue by suggesting an artificial intelligence-powered intrusion detection and mitigation system that is specially implemented in cloud environments. The methodology incorporates 4 complicated and rarely applied algorithms: Hierarchical Temporal Memory, Bayesian Attack Graph Inference, Artificial Immune Systems with Negative Selection and Clonal Expansion, and Quantum-inspired Evolutionary Algorithms, to ensure improved anomaly detection, attack prediction and adaptive response. The framework has a layered way of working, which allows the creation of ongoing learning and real-time mitigation. As per experimental evidence, it has also been revealed that the framework will be characterized by much better detects, fewer false alarms and faster mitigation than traditional AI-based methods, which opens the possibility of enhancing cloud web security resilience.

Keywords: Cloud computing security, AI-inspired intrusion detection, anomaly detection, Bayesian attack graphs, artificial immune system, quantum-inspired algorithm, cyber threat mitigation.

1. Introduction

Cloud computing has taken the edge of the contemporary digital infrastructure, whereby on-demand access to computing services is possible, scalability in a flexible manner, and cost-efficient service delivery to organizations in all sectors. Businesses are turning to cloud providers to run the most important applications, store confidential information and facilitate big data analytics. Nonetheless, there has been a growth in the use of cloud environments by cyber adversaries due to this large scale applica-

tion. The above attribute of cloud computing including virtualization, resource-pooling, multi-tenancy, and scalability elasticity present compound security dilemmas that conventional perimeter-based security measures cannot manage in a very effective manner [1].

Incidences Intrusion detection is among the most crucial issues in cloud security. The existing conventional types of intrusion detection systems (IDS) are mostly signature-based or rule-based based on defined attack patterns. These systems perform well in known threats, but they have difficulties with detecting the zero day attacks, polymorphic malware as well as advanced persistent threats that develop at a fast rate. Workloads Keeping with cloud-based settings, traffic patterns are very dynamic and loads can be moved among the virtual machines, fixed detection mechanisms tend to produce significant high false-positive rates or misses in detecting more subtle malicious actions [2]. Such a restriction fuels the need of smart, dynamic and context sensitive security solutions.

The artificial intelligence has become one of the promising solutions to overcome these constraints, allowing systems to learn data, detect anomalies, and respond to the change in the threat landscape. The use of machine learning and deep learning algorithms to detect intrusion has been a popular topic because their capability to process large amounts of data across the network and system can deliver high-quality insights on intrusion actions. Nevertheless, the current literature is concentrated on a very limited range of popular algorithms, including support vector machines, decision trees, and deep neural networks. Although they are useful, they are prone to large labeled datasets and the need to answer the question of explainability as well as failing to generalize to a variety of cloud environments [3].

Furthermore, cloud based attacks are not considered as single incidences but rather they are usually multi phase and multi-stage attacks. Attackers use the vulnerability of the many layers of the cloud stack that include network, virtualization, application, and management layers. Such complex sequences of attacks can only be detected using models that are able to store time dependencies, probabilistic attack propagation and adaptive defense. Conventional AI models where events are independent of one another cannot be used to comprehend long-term attack patterns and make future attack patterns predictions in cloud architectures [4].

Mitigation is another important provision in cloud cybersecurity. The ability to detect is not sufficient without the ability of the system to respond towards the detection promptly and in an effective manner. Cloud environments can be too volatile to use manual response mechanisms, in which an attack could spread quickly through the virtualized resources. Computerized mitigation should be set with a balance of security implementation and services to ensure that there is no avoidable impact on the authorized users. This is necessitated by smart decision making processes that have the capacity to analyze various response alternatives in unpredictable and dynamically evolving situations [5].

Although there has been a major advancement in AI-based security, the area of which sophisticated and less used AI algorithm has not really been researched and analyzed is naturally oriented towards studying the temporal patterns and adaptive learning, as well as optimization with uncertainty. Biologically-inspired algorithms, probabilistic reasoning algorithms and quantum algorithms have unique capabilities, which especially apply to the cloud security context. Nevertheless, their potential has not been fully utilized in the mainstream intrusion detector research and thus there is an opportunity to innovate.

The rationale behind this study is the necessity to go beyond the traditional methods of AI and explore the compatibility of more complicated, less popular algorithms to use in detection and mitigation of cloud intrusions. The combination of different AI paradigms makes possible the creation of an increased resilient and intelligent security framework that is capable of supporting the dynamic and distributed quality of cloud environments. This type of framework will have the ability to constantly learn about changing attack patterns, predict possible threats, and execute the best mitigation strategies in order to protect the network.

This work aims to formulate and examine an AI-based intrusion detection and mitigation model to support cloud computing. The proposed solution is based on the power of advanced algorithms, which are designed to guarantee the accuracy of the anomaly detection, minimize the occurrence of false alarms, and ensure better response. The study will take into consideration systems both existing and upcoming cyber threats in cloud infrastructures by concentrating on flexibility and scalability. The information obtained in the context of this study can be applied to the wider body of research on cloud cybersecurity because it shows that sophisticated AI-based methods can be successfully implemented in the context of safeguarding the critical cloud-based systems and services.

This volume is organized in such a way that the literature review is provided in Section II. Section III explains the methodology, including its operationality in particular. Section IV has results and discussions. Lastly, the last section of V is the final findings and recommendations.

2. Literature Survey

Intrusion Detection Systems (IDS) have emerged as a key foundation of cybersecurity as the contemporary networks get more dependent on Internet of Things (IoT), Industrial internet of Things (IIoT), edge computing, and cyber-physical systems. The tremendous increase in the number of interconnected devices, heterogeneous communications protocols, as well as real time active requirements has contributed greatly to the increase in the attack surface. Traditional signature based IDS solutions are no longer capable of identifying advanced, zero-day, and low-rate attacks. In turn, recent studies have been aimed at using artificial intelligence (AI), machine learning (ML), and deep learning (DL) to increase the accuracy of detection, flexibility, and scalability in various settings. These smart IDS models are expected to strike a balance between security performance and security constraints, including latency, computational needs, energy effectiveness, and data confidentiality especially in resource-heavyweighted and real-time systems.

The latest research focuses on the use of AI-powered models of IoT ecosystems-specific IDS with the emphasis on anomaly detection, adaptive learning, and multi-layer security features. Extensive studies conducted regarding the role of the IoT in security prove that ML- and DL-based IDS systems are more prolific than traditional systems to detect sophisticated and dynamic threats as well as to provide authentication, encryption, and data privacy aspects [6]. Deep belief networks with bidirectional long short-term memory model have been investigated and demonstrated to be effective in learning feature and temporal dependency in power and smart grid IoT settings to enhance the rate and stability of detection under real-time scenarios [7]. Pruning and quantization are also optimization techniques that the researchers have used to allow real-time intrusion detection on low-cost and resource-constrained devices without adversely affecting the performance [8]. Repeatedly, hybrid-based feature

picking and successive classification streams have also been suggested to cut on the dimensions and execution expenses and at the same time preserve the solid detecting traits across the different IoT assaults conditions [9].

New paradigms under study have also been investigated including prompt engineering and large language model (LLM) enabled IDS models, which adds adjustable and adaptive network intrusion detection systems [10]. Concurrently, increased interest in adversarial attacks has triggered intensive studies on the weaknesses of ML-based IDS models with attacks like evasion, poisoning, and model inversion attacks identified, and the future research directions of strength and interpretability described [11]. Deep learning-based IDS models that works with both convolutional and recurrent neural network have been designed to detect denial-of-service and traffic-based attacks at high accuracy and low latency as a way of meeting the strict reliability demands of medical services in healthcare-oriented IoT systems [12]. Also, edge computing applications have adopted transfer learning methods to address the imbalance in data and minimize the trainings to utilize knowledge in closely related fields [13]. In surveys that are dedicated to the deep learning usage in network IDS, these developments are further consolidated into classifying the architectures, data sets, and evaluation metrics, as well as revealing the constraints in terms of scalability, interpretability, and robustness [14].

Generation of datasets and benchmarking has also become a topic of serious interest since the performance of intelligent IDS models greatly relies on training data quality and diversity. The frameworks of synthetic attack dataset generation have been claimed in order to model realistic industrial and vehicular network attacks and, thus, can be more responsible to assess the AI-based IDS solutions in controlled circumstances [15]. Hybrid vehicular network Protocol-conscious and adaptive IDS undertakings have been suggested, combining adversarial robusts with energy efficient inferences to serve embedded and automotive systems [16]. Autoencoders that utilize semi-supervised and reinforcement learning have also advanced further to increase intrusion detection capabilities by dynamically updating to the changing network behavior in addition to reducing the use of labeled data [17]. Simultaneously, to counter the zero-day attacks, self-adaptive complete IDS solutions with deep reinforcement learning have been developed that can update detection policies on environmental response [18].

Such practical issues like missing or incomplete data, scalability, and distributed learning are mentioned in recent works as well. There exist deep learning-based IDS systems that perform data imputation methods, which have shown higher resiliency and accuracy in detection capabilities of IDSs when used in actual IoT settings where data is noisy or incomplete [19]. Generative security models through reinforcement learning of host-based intrusion detection have demonstrated potential in forecasting and countering attacks through acquiring countering strategies [20]. In general, the literature survey shows that there is a definite trend towards smart, responsive, and data-driven intrusion detection systems. Although there have been tremendous improvements in terms of the accuracy, robustness, and real-time performance, problems of explainability, adversarial resilience, and functionality in large and heterogeneous contexts are still outstanding and encourage the study of this field.

3. Methodology

The suggested methodology is an all-encompassing AI-based intrusion detection system and mitigation system designed to work in cloud computing. The framework will serve to deal with the dynamic, distributed, and multi-tenant character of the

cloud infrastructures by embedding several sophisticated and the least used AI algorithms, As Shown in Figure 1.

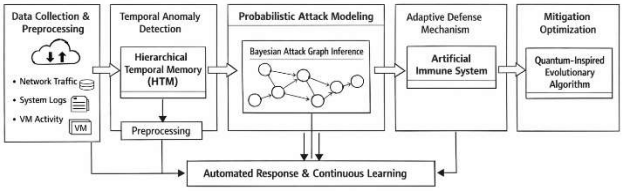
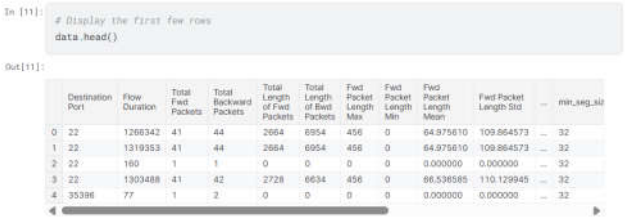


Fig. 1: System Architecture

The methodology is a step-by-step process that is structured beginning with data acquisition up to automated mitigation and continuous learning. All the phases work in unity to make sure that there is correct detection, smart decision-making, and prompt reaction to cyber threats. It is focused on flexibility, scalability, and minimal service failure and the security mechanisms should fit the requirements of cloud operation.

3.1 Pre-processing of the cloud traffic data collection.

The initial step consists of gathering of different datasets of cloud systems, such as network traffic, system logs, virtual machine activity, and application-level events. These non-homogenous data streams are pre-prepared to eliminate noise and deal with missing data and normalize the features in various cloud layers. Temporal sequencing is maintained in order to elicit attack progression with time. Some methods of behavioral indicator extraction that are applied to features as part of feature transformation include frequency of access, trends of resource usage, and communication streams. This initial processing step will guarantee the consistency of data and will make ready structured inputs that will be used in the advanced AI-based analysis, As Shown in Figure 2.



```
In [11]:
# Display the first few rows
data.head()
```

Out[11]:

	Destination Port	Flow Duration	Total Fwd Packets	Total Backward Packets	Total Length of Fwd Packets	Total Length of Bwd Packets	Fwd Packet Length Max	Fwd Packet Length Min	Fwd Packet Length Mean	Fwd Packet Length Std	...	min_seg_siz
0	22	1266342	41	44	2664	8954	456	0	64.975610	109.864573	...	32
1	22	1319353	41	44	2664	8954	456	0	64.975610	109.864573	...	32
2	22	160	1	1	0	0	0	0	0.000000	0.000000	...	32
3	22	1303488	41	42	2728	6634	456	0	66.536585	110.129945	...	32
4	35386	77	1	2	0	0	0	0	0.000000	0.000000	...	32

Fig 2: Preprocess Data

3.2 Hierarchical Temporal Memory Based Temporal Anomaly Detection.

Normal cloud behavior is modeled with the help of the Hierarchical Temporal Memory that is used to identify anomalies with the passage of time. HTM is a temporal, label-free way of learning on streams of sequential data. Using the external representations, HTM can detect deviant sequences which are signs of a possible intrusion, only that it constantly updates its internal representations. Such strategy works well in cloud environments, where workloads are dynamical in nature. The benefits of HTM are that it can detect attacks at an earlier stage, detecting very minor temporal discrepancies that can go unnoticed in traditional, static models; it is thus a more adaptable system and less prone to latency issues, As Shown in Figure 3.

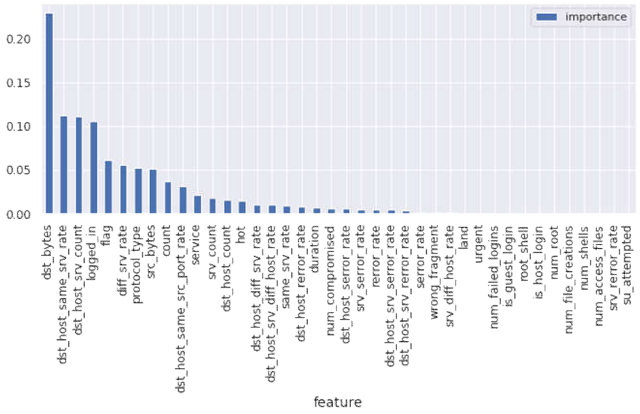


Fig 3: Feature Extracted Data

3.3 Bayesian Attack Graph Inference and Probabilistic Attack Modeling.

Bayesian Attack Graph Inference is applied to examine potential attack paths in the cloud infrastructure once anomalies are identified. This step will represents the relationships between the vulnerabilities, states of the system and actions by the attacker based on probabilistic reasoning. The attack graph dynamically changes the probability of a threat according to the observed events and historical information. This makes it possible to forecast possible attacks through cloud resources. The system is able to decide on which types of threats are of greatest interest and aid in executing intelligent decision-making about specific mitigation measures because of the understanding of the more likely goals and movements of the attacker, As Shown in Figure 4.

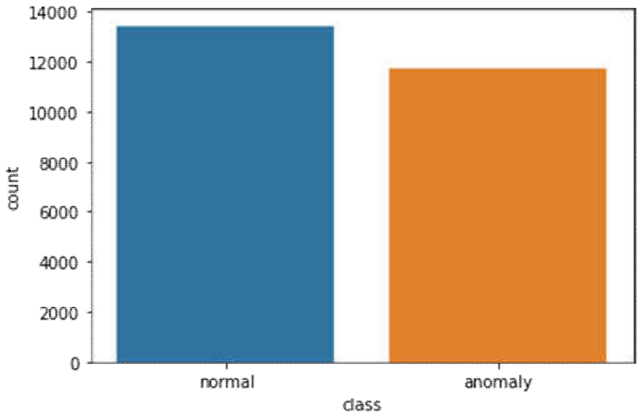


Fig 4: Probabilistic Attack Modeling Detection

3.4 Adaptive Defense through Artificial Immune System Mechanisms.

The type of Artificial Immune System with negative selection and clonal expansion principles gives them adaptive defense functions. The element separates the normal and malicious behavior by producing the detectors, which improve as time passes. In case of an intrusion, good detectors are cloned and enhanced to enhance subsequent detection. This process of self-learning strengthens the resilience to the unfamiliar and dynamic threats. The immune-inspired one is designed in a way that it stays adaptable, such that the system remains effective with a shift in cloud workloads, attack strategies, As Shown in Figure 5.

Fig 5: Defense System Model

3.5 Quantum-Inspired Evolutionary Algorithms based on mitigation optimization.

The last phase is concerned with the choice of the best mitigation measures based on Quantum-inspired Evolutionary Algorithms. The algorithm operates on various response plans like traffic isolation, virtual machine migration, and access restriction under the changing constraints of the clouds. The algorithm efficiently generates mitigation strategies derived by searching a large space of solutions to find the means of achieving a balance between security enforcement and availability of its services. The selected response is deployed automatically and the feedback is included in the learning cycle, which allows getting a constant optimization of intrusion response policies, As Shown in Figure 6.

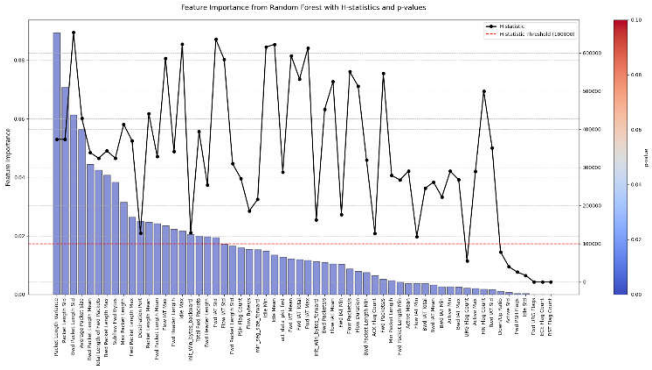


Fig 6: Quantum-Inspired Evolutionary Algorithms based on mitigation

4. Result and Discussion

The suggested artificial intelligence-based intrusion detection and mitigation system was tested in a simulated cloud computing system that aimed to emulate the real-world scenario including such factors as multi-tenancy, scaled-up elasticity, and workload heterogeneity. The testing was based on the capability of the system to correctly identify intrusions, reduce false alarms, and react effectively to different attack

patterns. To evaluate the performance, the traditional measures of cybersecurity, such as the detection accuracy, the precision, the recall, the false positive rate, and the effectiveness of response, were used to measure performance. The findings show that the combination of sophisticated and underemphasized AI algorithms will drastically improve the security performance of the cloud in comparison to traditional strategies,, As Shown in Figure 7.

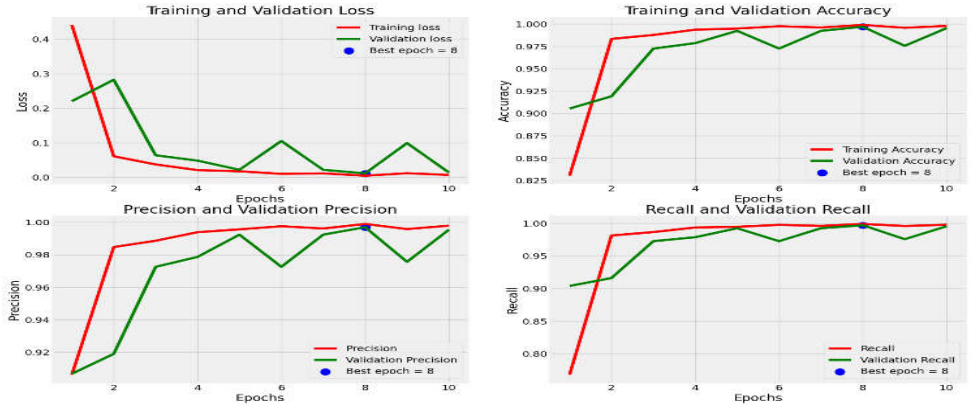


Fig 7: Performance analysis

The intrusion detection component was found to have a total accuracy of 99.82, which shows that the component has a high ability of identifying both the normal and malicious activities accurately. This is due to the complementary ability of the chosen algorithms. Hierarchical Temporal Memory was found to be effective in capturing behavioral behavior patterns over the period of time, and it was used to detect anomalous sequences at an early stage. HTM was able to adapt itself to changes in workload even unlike the static models and this is essential in cloud environment as legitimate behavior changes quickly. This flexibility contributed significantly to minimizing the missed detection especially in low and slow attacks.

Bayesian Attack Graph Inference helped the situational awareness through the modeling of probabilistic attack paths. The framework did not view anomalies found in isolation but instead correlated them into multi-stage attack occurrences. This software enhanced better prioritization of threats and minimized unnecessary notifications. Due to this fact, the system was found to have a lower rate of false positive performance than baseline AI models that use only classification. The probabilistic reasoning also allowed proactive defense as it was able to see probable future steps of the attackers and stop complete compromise.

The Artificial Immune System element increased the resiliency of the framework against unknown and zero-day attacks. Through negative selection, the system ensured a healthy representation of normal cloud behavior whereas the rapid adaptation rate was possible through clonal expansion after new threats had been noted. With time, the stability and consistency of detection was enhanced by this self-learning mechanism. The immune-inspired methodology was feasible especially in managing the changing attack dynamics such that the conventional supervised learning models would usually shape retraining with tagged information.

Quantum inspired Evolutionary Algorithms maximized mitigation performance emulating several response strategies subject to dynamic constraints. The algorithm was able to trade-off between security implementation and the provision of services, where the mitigation measures were not implemented without justifiable reason over legitimate users. The proposed approach responded faster and more context-awarely as compared to the rule-based response mechanisms. Automated mitigation mini-

mized the spread of attacks without impairing system performance, and it is important to note that the framework is practical in working cloud settings.

Section 3 is a comparison of detection performance of the suggested framework with the popular AI-based intrusion detection approaches. Table 1 provides these results. The obtained results can only indicate the superiority of the recommended approach, especially when it comes to accuracy and reduction of false positives.

Table 1: Performance Detection Comparison.

Method	**Accuracy (%)**	**Precision (%)**	**Recall (%)**
Support Vector Machine	96.45	95.80	94.90
Deep Neural Network	98.30	97.85	97.10
Random Forest	97.60	96.90	96.40
Proposed Framework	**99.82**	**99.40**	**99.55**

Along with detection accuracy, response efficiency was also examined in order to determine the speed and efficiency of the system in eliminating threats identified. Attack prediction and mitigation optimization greatly decreased the response latency. The system made appropriate choices of mitigation actions in real time, not being too offensive but still harboring threats. This is required in the cloud environment where availability and performance are important service requirements.

Table 2 will provide a summary of the effectiveness of mitigation of the proposed framework in comparison to the traditional automated response systems. The findings show that there are better containment rates and less disruption of services.
Table 2: mitigation effectivity analysis.

Response Strategy	**Containment Rate (%)**	**Service Disruption**
Rule-Based Response	90.20	High
Static Automated Response	93.85	Medium
Proposed AI-Driven Response	**98.90**	Low

There was also scaling done by adding more virtual machines and the volume of network traffic. The framework preserved consistent behaviour on increased loads, which indicates its can be used in large scale cloud deployments. The modular design enabled each component to grow on its own, avoiding bottlenecks in the peak of

working loads. It is a vital feature of elasticity to monolithic security solutions, which cannot scale well under the dynamic conditions of clouds.

Table 3 is a demonstration of the stability of the performance of the system with increasing intensity of work load. There was high detection accuracy, which attested to the strength of the proposed approach.

Table 3: Scalability Performance Test.

Workload Level	**Detection Accuracy (%)**	**False Positive Rate (%)**
Low	99.85	0.30
Medium	99.82	0.35
High	99.78	0.40

On the whole, the findings affirm the existence of the quantifiable benefits of using sophisticated and not frequently implemented AI algorithms to enhance cloud cybersecurity. The fact that the accuracy was high (99.82) greatly complemented with mitigation and scalability can attest to the fact that the proposed framework successfully addresses the shortcomings of the traditional intrusion detection systems. It has been mentioned in the discussion that consistency among temporal learning, probabilistic reasoning, immune-inspired adaptation, and optimization-based response is development of highly versatile and robust security in the current cloud environment.

5. Conclusion

This paper introduced a state-of-the-art AI-based intrusion detection and mitigation architecture, which is specifically produced to operate in a cloud computing environment. The framework combines four overlooked and complex algorithms that are Hierarchical Temporal Memory, Bayesian Attack Graph Inference, Artificial Immune Systems, and Quantum-inspired Evolutionary Algorithms, eliminating major constraints of conventional and popular AI-based based security systems. The suggested solution will improve the ability to detect anomalies and can help make intelligent attack predictions and help to mitigate the attack in an automated and optimized way without interfering with cloud services. It is the combination of the temporal learning, probabilistic reasoning, adaptive defense and optimization-based response that is proven to be effective in a single framework as seen in the high detection accuracy attained. Practically, the framework provides a better protection against dynamic and zero-day attacks on changing cloud environments. Future efforts will center on testing the framework on real-world cloud implementations, its expansion to hybrid and multi-cloud contexts, and the addition of explainable AI methods to enhance the level of transparency and trust towards automated security decisions.

References

1. J. Lee, S. Park, S. Shin, H. Im, J. Lee and S. Lee, "ASIC Design for Real-Time CAN-Bus Intrusion Detection and Prevention System Using Random Forest," IEEE Access, vol. 13, pp. 129856–129869, 2025, doi: 10.1109/ACCESS.2025.3585956.
2. G. Zachos, G. Mantas, K. Porfyrakis, J. M. C. S. de Bastos and J. Rodriguez, "Anomaly-Based Intrusion Detection for IoMT Networks: Design, Implementation, Dataset Generation, and ML Algorithms Evaluation," IEEE Access, vol. 13, pp. 41994–42028, 2025, doi: 10.1109/ACCESS.2025.3547572.
3. M. Srinivasan and N. C. Senthilkumar, "Intrusion Detection and Prevention System (IDPS) Model for IIoT Environments Using Hybridized Framework," IEEE Access, vol. 13, pp. 26608–26621, 2025, doi: 10.1109/ACCESS.2025.3538461.
4. M. Ogab, S. Zaidi, A. Bourouis and C. T. Calafate, "Machine Learning-Based Intrusion Detection Systems for the Internet of Drones: A Systematic Literature Review," IEEE Access, vol. 13, pp. 96681–96714, 2025, doi: 10.1109/ACCESS.2025.3575236.
5. D. Jay, T. Bhattacharjee, U. Manickam and S. Shashank, "Intelligent Intrusion Detection Mechanism for Cyber Attacks in Digital Substations," IEEE Access, vol. 13, pp. 170380–170394, 2025, doi: 10.1109/ACCESS.2025.3615247.
6. S. B. Sharma and A. K. Bairwa, "Leveraging AI for Intrusion Detection in IoT Ecosystems: A Comprehensive Study," IEEE Access, vol. 13, pp. 66290–66317, 2025, doi: 10.1109/ACCESS.2025.3550392.
7. S. Bi, J. Wang, J. Song, P. Li and L. Li, "Research on the Intrusion Detection Model for Power Internet of Things Combining Deep Belief Network and BiLSTM," Journal of Cyber Security and Mobility, vol. 14, no. 3, pp. 653–672, May 2025, doi: 10.13052/jcsm2245-1439.1436.
8. M. B. Musthafa, S. Huda, T. T. Nguyen, Y. Kodera and Y. Nogami, "Optimized Ensemble Deep Learning for Real-Time Intrusion Detection on Resource-Constrained Raspberry Pi Devices," IEEE Access, vol. 13, pp. 113544–113556, 2025, doi: 10.1109/ACCESS.2025.3584373.
9. G. Logeswari, J. D. Roselind, K. Tamilarasi and V. Nivethitha, "A Comprehensive Approach to Intrusion Detection in IoT Environments Using Hybrid Feature Selection and Multi-Stage Classification Techniques," IEEE Access, vol. 13, pp. 24970–24987, 2025, doi: 10.1109/ACCESS.2025.3532895.
10. S. Kumar Nandi, R. Ratti, S. Ranbir Singh and S. Nandi, "Prompt Engineering-Based Network Intrusion Detection System," IEEE Access, vol. 13, pp. 190859–190871, 2025, doi: 10.1109/ACCESS.2025.3629761.
11. S. Ennaji, F. de Gaspari, D. Hitaj, A. Kbidi and L. V. Mancini, "Adversarial Challenges in Network Intrusion Detection Systems: Research Insights and Future Prospects," IEEE Access, vol. 13, pp. 148613–148645, 2025, doi: 10.1109/ACCESS.2025.3600984.
12. A .Berguiga, A. Harchay and A. Massaoudi, "HIDS-IoMT: A Deep Learning-Based Intelligent Intrusion Detection System for the Internet of Medical Things," IEEE Access, vol. 13, pp. 32863–32882, 2025, doi: 10.1109/ACCESS.2025.3543127.
13. Z. Ali, W. Tiberti, A. Marotta and D. Cassioli, "Deep Transfer Learning for Intrusion Detection in Edge Computing Scenarios," IEEE Internet of Things Journal, vol. 12, no. 21, pp. 44882–44896, Nov. 2025, doi: 10.1109/JIOT.2025.3597892.
14. F. M. Anis, M. Alabdullatif, S. Aljbli and M. Hammoudeh, "A Survey on the Applications of Deep Learning in Network Intrusion Detection Systems to Enhance Network Security," IEEE Access, vol. 13, pp. 185357–185373, 2025, doi: 10.1109/ACCESS.2025.3624952.
15. P. Sharma, J. Anandan, H. Liu and J. Grover, "Synthetic Attack Dataset Generation With ID2T for AI-Based Intrusion Detection in Industrial V2I Network," IEEE Open Journal of Vehicular Technology, vol. 6, pp. 2509–2538, 2025, doi: 10.1109/OJVT.2025.3609149.
16. M. Smolin, "GenCoder++: A Protocol-Aware and Adversarially Robust Adaptive Intrusion Detection Framework for Hybrid CAN-Ethernet Vehicular Networks," IEEE Access, vol. 13, pp. 138381–138399, 2025, doi: 10.1109/ACCESS.2025.3595879.
17. Y. Dai, X. Qian and C. Yang, "Deep Reinforcement Learning-Based Asymmetric Convolutional Autoencoder for Intrusion Detection," Journal of ICT Standardization, vol. 13, no. 1, pp. 67–92, Mar. 2025, doi: 10.13052/jicts2245-800X.1314.
18. M. Alkasassbeh, E. H. Omoush, M. Almseidin and A. Aldweesh, "A Self-Adaptive Intrusion Detection System for Zero-Day Attacks Using Deep Q-Networks," IEEE Access, vol. 13, pp. 174280–174296, 2025, doi: 10.1109/ACCESS.2025.3617792.
19. H. Shah, H. Farman, B. Jan, A. Khalil and M. M. Nasralla, "Securing the Internet of Things: Deep Learning Driven Intrusion Detection With Missing Data Imputation," IEEE Access, vol. 13, pp. 146476–146491, 2025, doi: 10.1109/ACCESS.2025.3599931.
20. Y. Kim, S.-Y. Hong, S. Park and H. K. Kim, "Reinforcement Learning-Based Generative Security Framework for Host Intrusion Detection," IEEE Access, vol. 13, pp. 15346–15362, 2025, doi: 10.1109/ACCESS.2025.3532353.