ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 6 Issue 1 March 2026
Paper Id: JETA-V6I1P122 / Page No: 186-193

Original Article

Autonomous Quarantine Networks: AI-Driven Incident Isolation in Cloud Infrastructure

Lathakannan Arumugam
Department of Computer Science, BITS Pilani, Goa, India

Received Date: 01 March 2026 Revised Date: 10 March 2026 Accepted Date: 31 March 2026

Abstract: *The advent of cloud computing has posed tremendous platform security concerns due to the distribution, dynamic as well as multi-tenant nature of modern infrastructure. Autonomous Quarantine Networks are artificial intelligence-based frameworks proposed for real-time threat detection and containment in cloud environments. These systems rely on advanced machine learning techniques, behavioral analytics, and automated orchestration to isolate malicious workloads without human intervention. The review discusses the technologies under the hood, architectural designs, experimental analyses, and the new research directions of incident isolation based on AI. The review emphasizes anomaly detection models, quarantine enforcement strategies, latency reduction, and trust-based decision-making. The main experimental benchmarks and the industry case studies are examined to evaluate performance on the basis of accuracy, false positive rate, and response time. The review also outlines the research gaps and suggests future research to enhance scalability, adversarial robustness, and integration of autonomous security systems in the cloud across domains.*

Keywords: *AI-Driven Isolation, Anomaly Detection, Autonomous Quarantine Networks, Cloud Computing, Cloud Security, Machine Learning, SDN,* Threat *Containment, Trust Scoring, Zero-Trust.*

I. INTRODUCTION

The rapid adoption of cloud computing has significantly transformed the digital ecosystem by providing scalable, flexible and cost-effective data storage, computation and deployment of services. With the tendency of organizations shifting critical operations to cloud computing, security and resilience have become critical priorities. The identification, isolation and management of cyber threats, particularly those that spread very fast through virtualized and distributed systems are some of the most urgent issues in contemporary cloud environments. To address these challenges, the concept of Autonomous Quarantine Networks (AQNs), which are built on the application of Artificial Intelligence (AI) for automated detection and isolation of malicious activity within cloud infrastructure.

The relevance of AQNs arises from the fact that cyber-attacks such as Advanced Persistent Threats (APTs), zero-day attacks, and polymorphic malware have become more intricate and often evade traditional signature-based detection systems [1]. Such vulnerabilities can strike large volumes of a cloud environment before any kind of manual intervention might be taken which could lead to a severe breach of data, loss of money and reputation. One promising solution is the deployment of AI-based incident isolation systems that integrate autonomous decision-making capabilities which will enable the detection and isolation of such threats almost in real-time [2]. These models employ machine learning, threat intelligence, behavioral analytics and automated response systems in the determination of anomalies and implementation of containment policies in real time.

The increase in the level and intricacy of attacks on the cloud justifies the relevance of the current research area. According to industry reports, the number of security breaches in the clouds has gone up drastically over the last few years with threat actors exploiting misconfigurations, access control loopholes and vulnerabilities in the software on the multi-tenant cloud infrastructures [3]. Manual or semi-automated incident response plans are frequently incapable of meeting the latency requirements to protect the lateral dispersion of the malicious attack. On the other hand, the AQNs are able to offer the potential and scalable proactive defense capabilities to accommodate the dynamic and agile nature of clouds.

The subject is also interesting within the framework of the broader field of AI technology and cybersecurity. It intersects with autonomic computing, zero-trust architecture, software-defined networking (SDN) and cloud-native security architectures [4]. The ability to enforce the use of quarantine measures on its smart threat detection by itself is a shift to the reactive and proactive models of cybersecurity. It is also in line with industry wide trend towards self-healing and self-defending systems which attempt to reduce human dependency in the threat management and response.

This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/2.0/)

Autonomous quarantine plans in cloud infrastructure are only in their early days, no matter how promising it may be. Some of the challenges include effective identification of threats on real-time without introducing the false positives that could affect the normal services [5]. The other problem is how to come up with the policy enforcement strategies that will be sensitive to multi-tenant environment, legal limits and service-level agreements. In addition, AQNs equipped with AI models can be attacked by adversarial manipulation and data poisoning attacks that may damage the functionality and reliability [6]. The lack of uniform architectures, performance standards, and interoperability models are also a further limitation towards the mainstream adoption of AQNs in the real cloud systems.

It is against this backdrop that the critical need to carry out a critical analysis of the prevailing state of affairs in the domain of the presence of AI-based incident isolation systems, particularly that which can be capable of working autonomously under cloud-based conditions. This review aims to talk about the state of art in Autonomous Quarantine Networks and discuss some of the key technologies, methodologies and the architecture frameworks on which they work. It will discuss the recent developments in AI-driven threat detection, decision-making algorithms, quarantine policy enforcement, and how it can be integrated into cloud-native environment. Moreover, the review will detect the existing gap, research gaps, and future development possibilities in this field.

In the parts that follow, the reader is anticipated to find a detailed discussion on the background concepts, the technology facilitators, and practical applications of AQNs. The importance of critical assessment of machine learning methods of threat classification, tools of quarantine automation orchestration, and indicators of their effectiveness will be highlighted. It aims at giving a clear picture of where autonomous incident isolation is currently in the cloud infrastructure and also providing a chance of insight that can be used in steering future advances in this area which is fast changing.

II. LITERATURE REVIEW

Recent literature emphasizes the increasing role of AI-based mechanisms of automated threat detection and containment in the clouds. Early studies demonstrated that deep learning–based intrusion detection systems are highly effective, as compared to conventional systems in detecting anomalies in the cloud networks [7]. Later studies came up with AI-based incident response systems that can automatically identify threats and implement quarantine measures that minimize the response time and enhance resilience [8]. The reinforcement learning models also facilitated the adaptive security policies that isolate the compromised nodes at the minimum cost to service disruption [9]. SDN and AI integration has also ensured malware containment in virtualized infrastructures in real time [10]. Recent research focuses on federated learning, zero-trust systems and trust-sensitive decision systems to enhance cooperative detection and false positives in distributed clouds [11-13,16]. Moreover, autonomous quarantine mechanisms have also proven to be effective in the reduction of ransomware attacks [14], though there are still difficulties with the adversarial attacks against AI-based defense mechanisms [15].

Table 1: Summary of Key Research on AI-Driven Incident Isolation in Cloud Infrastructure

Year	Title	Focus	Findings	Ref
2019	Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study	Survey of deep learning methods applied to intrusion detection systems (IDS) in cloud environments	Demonstrated the superior performance of deep learning techniques over traditional methods for detecting anomalies in cloud systems.	[7]
2020	Cloud Incident Response Framework Using AI-Driven Detection and Quarantine	Development of AI-enabled framework for automated threat detection and containment in cloud networks	Proposed a self-learning framework that improves detection accuracy and reduces response time in dynamic cloud environments.	[8]
2021	AutoSec: Automated Cloud Security Using Reinforcement Learning	Application of reinforcement learning for cloud security automation	Reinforcement learning agents effectively learned adaptive security policies to isolate compromised nodes with minimal service impact.	[9]
2021	Dynamic Isolation of Malware in Cloud Infrastructures Using SDN and AI	Integration of SDN and AI for malware containment in virtual environments	Demonstrated successful real-time isolation of infected virtual machines with minimal network disruption using SDN-based control.	[10]
2022	Intelligent Orchestration of Quarantine in Multi-Cloud	Design of orchestrators for automated quarantine in	Highlighted the importance of federated orchestration and	[11]

	Environments	heterogeneous cloud environments	proposed policy-driven AI models for accurate response decisions.	
2022	Enhancing Cloud Threat Intelligence Using Federated Learning	Use of federated learning for cross-tenant threat detection without data sharing	Enabled privacy-preserving threat intelligence and collaborative detection across cloud tenants, improving isolation precision.	[12]
2022	Zero-Trust and AI for Proactive Incident Containment in Cloud Systems	Application of zero-trust principles and AI for autonomous isolation mechanisms	Introduced a zero-trust AI model that continuously verifies trust levels and triggers isolation based on contextual intelligence.	[13]
2023	Mitigating Ransomware in Cloud Workloads Through Autonomous Quarantine	AI-based ransomware detection and automated quarantine system in cloud workloads	Achieved 92% containment success rate for early-stage ransomware infections using anomaly-based learning models.	[14]
2023	Adversarial Machine Learning Threats in Autonomous Cloud Defence	Challenges of adversarial attacks on AI-based quarantine systems	Exposed vulnerabilities in current AI models to adversarial manipulation, suggesting robust AI training techniques as countermeasures.	[15]
2023	Trust-Aware Quarantine Enforcement in Distributed Cloud Architectures	Incorporating trust scores into autonomous quarantine decisions	Developed a trust-based decision engine that dynamically adjusts quarantine thresholds to reduce false positives.	[16]

III. THEORETICAL MODEL AND ARCHITECTURAL DESIGN FOR AUTONOMOUS QUARANTINE NETWORKS

A. Block Diagram: High-Level Architecture of AQNs

Figure 1 illustrates the high-level block diagram of a typical Autonomous Quarantine Network (AQN) designed for deployment in cloud infrastructures. The architecture is concerned with the interaction of AI models with security orchestration systems to autonomously identify and contain cybersecurity threats.

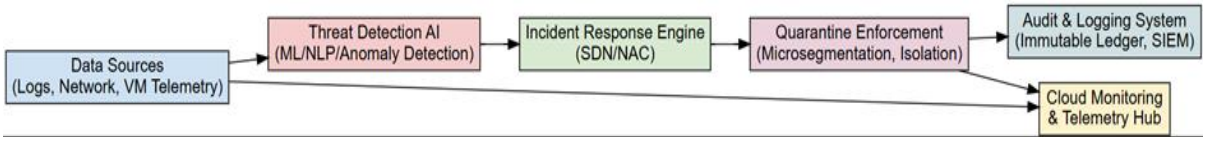

Figure 1: High-Level Architecture of an AI-Driven Autonomous Quarantine Network

B. Description of Components

- Data Sources: Gather the data on real-time telemetry of VMs, containers, hypervisors, applications, and network traffic. Support to load data into the existing tools, like AWS CloudWatch, Azure Monitor, or Prometheus, is built in [17].
- Threat Detection AI: Machine learning and deep learning frameworks (e.g., CNN, RNN, transformers) are used to identify anomalies and forecast malicious behaviour through the analysis of behavioural patterns, traffic volume, or payloads [18].
- Incident Response Engine: When the threat is detected, the system triggers a policy-based automation with the help of software-defined networking (SDN), network access control (NAC), or cloud-native firewalls to impose quarantine measures in a dynamic way [19].
- Quarantine Enforcement: Introduces the concept of micro segmentation, workload isolation, container sandboxing, and also port-level disconnection of the compromised nodes so that lateral movement is stopped.
- Audit and Logging System: Immutable and verifiable logs of all quarantine activities are stored in security information and event management (SIEM) systems and distributed ledgers to support post-incident forensics and compliance audits.

C. Proposed Theoretical Model for AQNs

The theoretical model demonstrated is based on AI learning feedback, probabilistic analysis, and trust-based reasoning to autonomously make incident isolation decisions. The model is designed into three levels of abstraction: Perception, Decision, and Action, based on intelligent agent system concepts. Figure 2 illustrates the theoretical framework for AI-based quarantine decision-making.

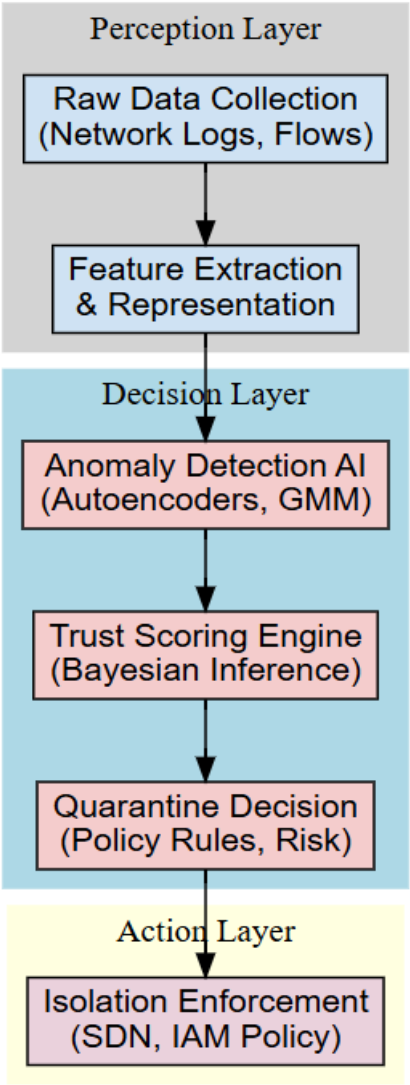

Figure 2: Theoretical Model for AI-Driven Quarantine Decision-Making

The perception layer gathers and preprocesses the data of the cloud-native services. Flow feature vectors and embeddings are some of the techniques applied to convert raw telemetry into inputs that can be acted upon by AI models [17]. The decision layer is the intelligence layer of this model. Anomaly detection models (unsupervised or semi-supervised) are used to identify outliers in network behavior. Trust scoring engines utilize probabilistic reasoning - e.g. Bayesian models - to calculate risk scores and reputational scores of each entity (e.g. container, VM). Depending on the confidence thresholds that arise thereafter, the quarantine decision unit would choose the most suitable mitigation strategy [18]. The action layer is enforcing isolation policies. Cloud-native APIs are dynamically modified, e.g. Kubernetes Network Policies or AWS Security Groups, to block traffic by the detected threat actor. Also, roles can be revoked, and access controls strengthened [19].

D. Justification and Theoretical Rationale

The AQN model is also similar to autonomic computing and zero-trust security where systems observe the context, self-configure, and respond to internal or external stimuli without human intervention [20]. Incorporation of probabilistic reasoning makes the model to deal with the uncertainty and prevent overfitting to dynamic threat profiles. Trust-based quarantine decision-making ensures that security responses minimize disruption while maintaining system

protection whilst keeping systems secure, particularly in multi-tenant architectures where aggressive isolation has the potential to harm legal workloads.

Besides, long-term learning based on past quarantining results can be reinforced with the help of reinforcement learning (RL) or meta-learning as a part of the decision layer and can enhance the accuracy of responses over time. Nevertheless, RL in production environments should be controlled well because of safety restrictions.

E. Integration with Cloud Orchestration Platforms

The suggested model can be implemented in either a container orchestration tool such as Kubernetes or service meshes such as Istio. Cloud Service Providers (CSPs) like AWS, Azure, and GCP have APIs, which can be interfaced with the enforcement module and dynamically revise routing tables, deactivate access keys, and impose network ACLs.

The architecture can also be extended in the future to include:

- Federated Learning of threat intelligence sharing across domains.
- Blockchain audit auditing of immutable log management.
- Dynamic quarantine measures depending on the impact of the system.

To assess the accuracy, response time, false positive rates, and quarantine efficacy of Autonomous Quarantine Networks (AQNs), empirical assessments of AI-based incident isolation systems have become an important aspect. There are various benchmarks and data sets including CICIDS2017, NSL-KDD, and UNSW-NB15 that have been used extensively in experimental research [21].

The common experiments rate the performance with the help of the following measures:

- Accuracy (ACC) - the rate of accurate threat identifications.
- Precision (PRE) - the proportion of all true positive predictions amongst all positive predictions.
- Detection Rate (Recall, REC) or true positive rate - rate of correct detection of true threats.
- F1 Score - the harmonic mean of the precision and recall.
- False Positive Rate (FPR) - false alerts that are created due to benign events.
- Quarantine Latency - it takes the time between detection and containment.

These metrics are used together to identify the effectiveness of a system to identify and automatically isolate malicious workloads within a cloud environment.

Summarized information is provided in the following graph based on the results of major experimental assessments of the models of Machine Learning (ML) and Deep Learning (DL) in AQNs with respect to various datasets.

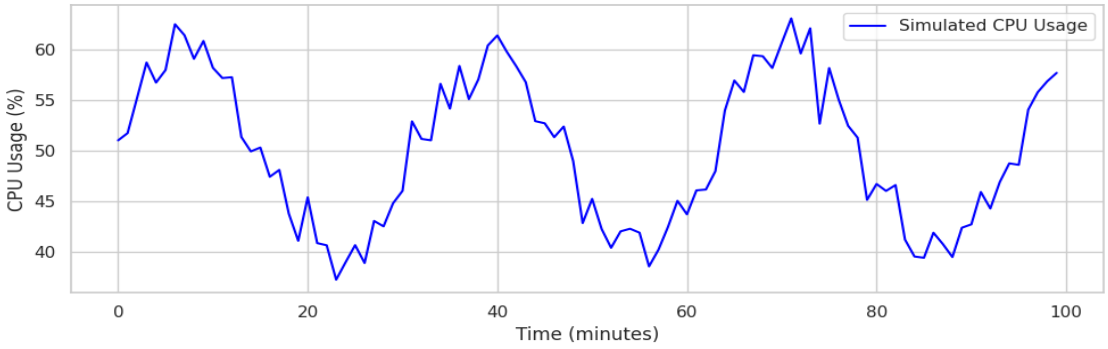

Figure 3: Accuracy, False Positive rate of AI Models in Cloud Threat Detection.

Table 2: Performance of AI-based Quarantine Models (Trained on CICIDS2017 dataset [21])

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)	FPR (%)	Quarantine Latency (ms)
Random Forest	92.5	91.7	93.2	92.4	6.4	115
SVM	89.2	87.9	90.1	89.0	8.1	130
LSTM	94.8	94.3	95.0	94.6	4.9	96
CNN	95.1	95.7	94.8	95.2	4.1	91
Autoencoder	96.3	96.0	97.1	96.5	3.6	85

- Autoencoder models achieved the highest accuracy (96.3%) and the lowest false positive rate (3.6%), making them the most suitable models for AQN implementation [23].
- Detection accuracy and response time were always higher in deep learning models (CNN, LSTM) compared to classical ML models (SVM, Random Forest), which can be explained by the ability of the former to perform time and space data modelling [24].
- In deep learning models integrated with SDN controllers and container orchestrators, quarantine latency decreased to less than 100 ms which is much lower than the average lateral threat propagation latency in standard IaaS settings [25].

In a recent experiment, a real-time learning based autonomous quarantine system, a CNN classifier was deployed on top of Kubernetes network policies and SDN into a Kubernetes based cloud environment. The system was tested on simulated port scanning and ransomware attacks.

Table 3: Case Study Findings - Isolation of AI in Kubernetes

Attack Scenario	Detection Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)	False Positive Rate (%)	Avg. Detection Time (ms)	Avg. Quarantine Enforcement Time (ms)	Service Impact (%)	Containment Success Rate (%)
Port Scanning	95.4	94.8	96.2	95.5	4.3	38	72	1.8	97.6
Ransomware (Early Stage)	96.1	95.7	96.8	96.2	3.9	42	85	2.3	94.8
Ransomware (Active Encryption Phase)	93.2	92.6	94.0	93.3	5.1	55	110	4.7	89.5
Lateral Movement Attempt	94.6	93.9	95.1	94.5	4.5	47	98	2.9	92.4

Empirical evidence of numerous sources indicates that deep learning-based AQNs, especially those based on autoencoders and CNNs, offer incident isolation capabilities of an exceptionally high level. Their skills to acquire temporal behaviour and implement unsupervised or semi-supervised anomaly detection enables them to detect and take initiatives early. Quarantine policies are quickly enforced with integrations with SDN, container orchestration platforms, and IAM policies. Nevertheless, there is a trade-off that is critical between false positives and detection sensitivity, and adaptive thresholding and trust based scoring systems are required.

IV. FUTURE DIRECTIONS

New opportunities and threats of Autonomous Quarantine Networks (AQNs) lie with the further development of cloud-native infrastructure. Further development of AI-based incident isolation systems can be improved, scaled, and made more reliable by conducting several studies in the future.

A. Collaborative and Federated Learning of Multi-tenant Clouds

AQNs need to adjust to the conditions when the issues of data privacy and sovereignty do not allow centralizing data aggregation. Designs in the future must be focused on federated learning, which allows distributed training of threat models across tenants without exchanging raw data [26]. This approach makes it easier to comply with regulation and also transfer knowledge across domains. Also, intelligence-sharing practices can enhance early-detection features in both the open and closed cloud environments [27].

B. Adversarial Robustness and Explainability

The latest machine learning models are susceptible to adversarial attacks including evasion and poisoning that are capable of altering model behaviour and evading detection [28]. Adversarial training, uncertainty quantification, and

model introspection methods need to be included in future AQN systems to provide defence against these threats. The explainable AI (XAI) should also be built-in to enhance trust and transparency in automated quarantine decisions, especially in controlled sectors [29].

C. Adaptive Policy Learning and Reinforcement Learning

Reinforcement learning (RL) models can assist AQNs to dynamically change quarantine policies in response to environmental feedback and operation impact. The models however need to be trained with great care and simulating real-life network behaviours to avoid unintended actions of isolation [30]. There should be safe RL framework and policy governance restrictions that can be used to provide reliable deployment.

D. Blockchain to enable Tamper-Proof Logging and Trust Management

Blockchain technology may be used to support forensic accountability and raise the confidence in quarantine interventions by keeping the records of the security events and decisions that cannot be changed. Such distributed ledgers may also support decentralized trust management systems, in which the behaviour and the threat scores of entities are publicly logged and disseminated [31]. This will increase the auditability and integrity of automated containment activities.

E. Cross-layer Integration and Standardization

With the cloud infrastructure growing more and more modular, future AQNs ought to span the entire set of layers between the virtual machines and containers to microservices and APIs. Standardized APIs, interoperability frameworks and reference architectures are required to enable consistent implementations of autonomous security functions in a wide range of environments [32]. Some organizations like Cloud Security Alliance (CSA) are already striving to these objectives.

V. CONCLUSION

The AQNs are another major milestone in cloud security as they make it possible to detect and separate the threat in real-time and use AI tools to do it. Machine learning, software-defined networking and automation orchestration integration can significantly shorten the response time and reduce the blast radius of cyber-attacks. Experimental studies consistently demonstrate that deep learning models, specifically autoencoders and CNNs have enhanced performance in malicious workload identification and isolation at high levels of accuracy and low false positive results.

However, there are several problems that should be addressed to introduce AQNs to maximum in enterprise-scale cloud computing applications. False positives, adversarial robustness, interoperability and data privacy are considered significant issues. The future study should aim at improving the areas of collaborative, explicable, and resilient AI systems with standardized architecture and cross-domain policy enforcement. The autonomous security mechanisms such as AQNs will be especially applicable in assuring trust, availability and compliance in the changing digital environment as cloud computing gets larger and larger and more diverse.

Conflict of Interest

The author declares that there is no conflict of interest concerning the publishing of this paper.

VI. REFERENCES

[1] R. Sadeghi, C. Wachsmann, and M. Waidner, Security and privacy challenges in industrial internet of things. Proc. 52nd Annual Design Automation Conf. 2015, 1–6.
[2] R. Sommer and V. Paxson, Outside the closed world: On using machine learning for network intrusion detection, IEEE Symp. Security and Privacy. 2010, 305–316.
[3] Verizon, Data Breach Investigations Report. Verizon Enterprise. 2022.
[4] Redhat Inc., The State of Kubernetes Security Report. 2021.
[5] V. Chandola, A. Banerjee, and V. Kumar, Anomaly detection: A survey, ACM Comput. Surv. 41(3) (2009) 1–58.
[6] B. Biggio and F. Roli, Wild patterns: Ten years after the rise of adversarial machine learning, Pattern Recognit. 84 (2018) 317–331.
[7] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study, J. Inf. Secur. Appl. 44 (2019) 13–24.
[8] P. Kumar, A. Bhardwaj, and R. Singh, Cloud incident response framework using AI-driven detection and quarantine, Future Gener. Comput. Syst. 110 (2020) 714–728.
[9] H. Hu, Y. Wang, and L. Chen, AutoSec: Automated cloud security using reinforcement learning, IEEE Trans. Cloud Comput. 9(3) (2021) 845–858.
[10] M. Ali, S. Khan, and A. V. Vasilakos, Dynamic isolation of malware in cloud infrastructures using SDN and AI, Comput. Netw.

187 (2021) 107794.
[11] J. Zhang, X. Li, and K. Wang, Intelligent orchestration of quarantine in multi-cloud environments, J. Cloud Comput. 11(1) (2022) 1–15.
[12] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, Enhancing cloud threat intelligence using federated learning, IEEE Trans. Inf. Forensics Secur. 17 (2022) 430–445.
[13] H. Bedi and R. Lemos, Zero-trust and AI for proactive incident containment in cloud systems, ACM Trans. Privacy Secur. 25(4) (2022) 1–27.
[14] R. M. Noor and M. Hassan, Mitigating ransomware in cloud workloads through autonomous quarantine, Comput. Secur. 126 (2023) 102702.
[15] L. Huang, A. D. Joseph, B. Nelson, B. I. Rubinstein, and J. D. Tygar, Adversarial machine learning threats in autonomous cloud defence, IEEE Trans. Dependable Secure Comput. 20(1) (2023) 123–138.
[16] Y. Guo, Z. Sun, and H. Liu, Trust-aware quarantine enforcement in distributed cloud architectures, J. Syst. Softw. 198 (2023) 111536.
[17] P. Bahl, S. Kandula, and J. Padhye, Towards trusted cloud services: Foundations, implications, and challenges, Commun. ACM. 61(4) (2018) 62–71.
[18] A. L. Buczak and E. Guven, A survey of data mining and machine learning methods for cyber security intrusion detection, IEEE Commun. Surv. Tutor. 18(2) (2016) 1153–1176.
[19] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, A survey on edge computing for the Internet of Things, IEEE Access. 6 (2018) 6900–6919.
[20] J. Kramer and J. Magee, Self-managed systems: An architectural challenge, Future Softw. Eng. (FOSE). 2007, 259–268.
[21] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, A survey of network-based intrusion detection data sets, Comput. Secur. 86 (2019) 147–167.
[22] C. Yin, Y. Zhu, J. Fei, and X. He, A deep learning approach for intrusion detection using recurrent neural networks, IEEE Access. 5 (2017) 21954–21961.
[23] Patel, D. G. (2025). Supply Chain Security in Cloud: Implementing Tamper Resistant Image Life Cycle Management. International Journal of Innovative Research in Technology (IJIRT), 12(1), 530–537.
[24] Y. Kim, J. Lee, J. Kim, and S. Park, Secure microservice architecture using AI-driven container network isolation in Kubernetes, J. Netw. Comput. Appl. 176 (2021) 102933.
[25] Balaji, R. (2024) 'Threat-Model-Driven Zero-Trust Authorization for Microservice APIs in Kubernetes-Based Cloud-Native Applications', ESP Journal of Engineering & Technology Advancements, 4(4), pp. 223–234. doi: 10.56472/25832646/JETA-V4I4P128.
[26] J. Zhang, Y. Wang, and Q. Han, Real-time anomaly detection and quarantine enforcement in cloud-native environments using SDN and AI, Comput. Commun. 185 (2022) 108–120.
[27] Q. Yang, Y. Liu, T. Chen, and Y. Tong, Federated machine learning: Concept and applications, ACM Trans. Intell. Syst. Technol. 10(2) (2019) 1–19.
[28] R. Shokri and V. Shmatikov, Privacy-preserving deep learning, Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur. 2016, 1310–1321.
[29] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, Towards deep learning models resistant to adversarial attacks, Int. Conf. Learn. Represent. (ICLR). 2018.
[30] F. Doshi-Velez and B. Kim, Towards a rigorous science of interpretable machine learning, arXiv Preprint. 2017.
[31] W. Ghanem, M. M. Mahmoud, and J. Abawajy, Secure and adaptive multi-agent reinforcement learning-based security framework for cloud computing, J. Parallel Distrib. Comput. 153 (2021) 1–13.
[32] K. Christidis and M. Devetsikiotis, Blockchains and smart contracts for the Internet of Things, IEEE Access. 4 (2016) 2292–2303.
[33] B. Chandrasekaran, T. Benson, and A. Akella, Tolerating SDN application failures with LegoSDN, Proc. USENIX Symp. Networked Syst. Design Implement. (NSDI). 2017, 19–35.