International Journal of Multidisciplinary Research and Growth Evaluation.

Adaptive Machine Learning Frameworks for Real-Time Threat Detection in Cloud Environments

Amjed Abbas Ahmed
[1] Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), Bangi 43600, Malaysia
[2] Department of Computer Techniques Engineering, Imam Al-Kadhum College (IKC), Baghdad, Iraq

* Corresponding Author: **Amjed Abbas Ahmed**

Article Info

ISSN (online): 2582-7138
Volume: 06
Issue: 04
July - August 2025
Received: 18-05-2025
Accepted: 19-06-2025
Published: 05-07-2025
Page No: 223-229

Abstract
The fast implementation of cloud computing in the various industries has revolutionized the digital world but at the same time posed sophisticated security issues. Cloud environments are dynamic in nature (distributed architecture, short life time resources, variable workload). Static security systems that act upon and refer to static rules as well as systems that are signature-based have become outdated in safeguarding against dynamic cyber attacks that are real-time. Following the trend of attackers using sophisticated approaches such as polymorphic malware, intelligent intrusion, and automated attack framework, the requirement of intelligent, scalable, and responsive security frameworks has become essential. Adaptive Machine Learning (AML) frameworks become an intriguing approach, as it allows to detect threats in real-time by learning and adjusting to the changes of patterns, behaviors and threats environment in cloud environments. This paper entails an in-depth examination of the AML technique which shall be applied to real-time cloud security. The review explores the most salient components of AML which include incremental learning, online learning, ensemble modeling, and drift detection, which can help AML systems stay steady over known and emerging risks. The common challenges of application of AML such as concept drift, high false positives, data privacy limitations as well as scalability issues are also addressed in the paper. In addition, it examines industry trends, new opportunities such as federated learning and explainable AI, and presents upcoming research topics, such as quantum-enhanced machine learning to be used in cybersecurity. The results reaffirm that AML is no longer a mere reactive measure but also a proactive, mandatory component used to protect present-day cloud architectures against a dynamically changing cyber-threat environment.

DOI: https://doi.org/10.54660/.IJMRGE.2025.6.4.223-229

Keywords: Cloud Security, Adaptive Machine Learning, Concept Drift, Real-Time Threat Detection, Online Learning, Anomaly Detection, Cybersecurity, Cloud Computing

1. Introduction

Digital transformation [1] fueled by cloud computing has resulted in an explosion in data generation, use of services and digital interconnectivity. The necessitating infrastructures of high availability, scalability and reliability has become ever so dedicated as organizations transit significant concentrations of their workloads to the cloud [2-4]. Nevertheless, elasticity, multi-tenancy, and worldwide distribution, which makes cloud computing so attractive, poses major challenges in terms of cybersecurity. The cloud service diversifies the area of attack exponentially, allowing cyber criminals to target and exploit vulnerabilities in more sophisticated and large scales.

Cybercriminals are increasingly automating attack tools, malware that uses artificial intelligence and botnets that can attack even a minor misorganization or security flaw [5-7]. In addition, security is also complicated by the incorporation of cloud services, IoT, mobile devices, and edge computing. These dynamic interconnected systems are dynamic in nature and therefore, it is impossible to keep up the fast changes in terms of workload, configurations, and user behaviors that are the characteristics of cloud environments using traditional security solutions.

The signature-based security technologies are in use that are based on the database of known threats. Although they are capable of defending against the former known attack vectors, they are incapable of dealing with zero-day vulnerabilities or advanced persistent threats (APTs). The behavioral analytics gives some increment but even that is not without struggle when patterns change fast or when there is a legitimate change in a behavior like during an application scaling or load balancing in the cloud [8-10].

The further rise in the usage of microservices, serverless, and containerized solutions further adds to the problem of anomaly detection [11]. As the parts spawn and close dynamically, the fixed security measures fail to notice fleeting evil procedures or side-to-side progress inside containerized enterprises.

Adaptive Machine Learning (AML) is an answer to these difficulties, as it presents a shift in paradigm. Automated machine learning systems [12-14] is specifically tailored to be run in real-time, with continual learning based on representing incoming data streams and adapting their internal models in real-time and dynamically with every change in patterns. In contrast to traditional models which must be trained once and deployed, AML models are never deployed, but instead constantly updated based on new information, solving the concept drift-problem, of gradually or instantaneously shifting data distributions with time [15].

The main objective of the paper is to discuss the ability, architectures, methodologies and the challenges that are related with the AML frameworks of cloud threat detection. This review aims to provide benefits both to academic researchers and to industry practitioners interested in implementing scalable security solutions to the real-time cloud environment, by reviewing various ways that these systems detect, adapt and respond to cybersecurity threats in real-time cloud environments.

2. Literature Review

2.1 Traditional Security Approaches

Static and perimeter based networks [16] are what conventional security mechanisms were built against. An example is firewalls which come in as gatekeepers between internal trusted networks and external untrusted sources. Other techniques such as rule-based or signature techniques of intrusion detection using Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are to identify known threats. But in a cloud surroundings, these tools will be very limited because no visible boundaries can be drawn within a network.

In addition, cloud infrastructures [17] often have ephemeral workloads such as virtual machine, containers, or serverless functions, which are launched and terminated in minutes or seconds. This volatility makes no rules applicable. Conventional security strategies were never intended to track the assets that have a shorter life span than the security audit time required to conduct a manual security audit. Most of the security tools available have scalability issues. The firewall rule that is successful in an on-site data center may become a bottleneck in cloud environments that may be producing gigabytes of data within each second. False positives fluster IDS tools in cloud systems because genuine, though unpredictable, workload distributions frequently elicit alerts generated by events that would be ordinary in evolving cloud systems. The use of the familiar patterns of attack also limits the traditional systems. Since signature-based detection fails at identifying newer malware, this approach becomes less effective as cyber adversaries use polymorphic malware that is ready to change their code structure anytime. Similarly, DDoS mitigation devices can fail in form of highly-advanced attacks that are mixed in with normal traffic like low-and-slow attacks or application-layer DDoS [18].

Another complication stems out of the shared and distributed characteristics of cloud infrastructures. These types of attacks are possible avenues of attack that attackers can exploit because of the cloud elastic nature enabling them to spawn numerous resources in cloud provider. Under these conditions, perimeter-based tools will not provide any measure of defense because the attack is literally inside the perimeter.

2.2 Machine Learning in Cloud Security

Machine learning (ML) [19] technology as applied to cloud security marks a great step up as compared to signature-based systems. The supervised learning models are trained with historical data that are marked either as benign or malicious. In these models, characteristics of the network traffic, user activity, or system logs are further defined to learn boundaries of classification on what is traced to be a normal operation and what is actually a threat.

Existing ML models [20], however, perform significantly better the better training data are achieved, which is often both costly and time-consuming. The imbalance of cybersecurity data is the well-known problem with much fewer attacks than non-malicious traffic examples. The result of this skew is models that are somehow too sensitive (high false positive) or over-conservative (fail to detect real attacks).

Moreover, the conventional ML models [21] assume the existence of a fixed distribution of data, which is seldom met in the cloud. As an example, a successful anomaly detection model may fall behind after an important software update causes a SaaS application to behave differently.

Unsupervised models, like clustering or dimensionality reduction models (e.g. PCA, t-SNE) [22] provide some protection against adversaries, in that they will identify outliers, but may not provide them in a fashion useful as actionable threat detection. There are always false positives that cause too much noise to security analysts and SOCs (Security Operations Centers).

To capture more complex patterns in cybersecurity [23-25] data, deep learning strategies have been introduced, which include, Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs). Although they are useful in certain applications, the models are computationally and data-intensive, which does not fit in limited environments such as real-time application.

2.3 Emergence of Adaptive Learning

The below issues of the traditional security systems and the

static ML model [26] are tackled through adaptive learning. Using models which are learned incrementally, AML systems can update their knowledge of network behavior and threat signatures with the environment. Studies have developed different AML frameworks and one of them is MOA (Massive Online Analysis) that offers an expandable platform by which to assess stream-based learning algorithms in cybersecurity. Equally, River, which is a similar framework allows online machine learning with tools that are made to deal with one piece of data at a time, which makes it favorable to real-time applications.

Nonstreaming forms of many classifiers [27], [28] such as Naive Bayes, Decision Trees and Support Vector Machines have also been created to accommodate data streams. Thes models are supposed to modify weights, probability distributions or decision boundaries with respect to every new data point without a need to be retrained again.

Additional capabilities of AML are brought about by the introduction of drift detection mechanisms. Other more dynamic methods such as ADWIN are used to maintain a window of the latest data and optimal size of the window is dynamically updated according to the variance of the data stream. In case a significant change is identified, the model adjusts its parameters by eliminating the possibility of accuracy decline.

The significance of AML is also supported by its inclusion in the commercial cloud security software. As an illustration, AWS GuardDuty constantly learns new models of threat detections with streaming VPC flows, DNS queries, and CloudTrail events, which shows the importance of AML in contemporary cybersecurity practices [29].

3. Methodologies for Adaptive Threat Detection

3.1 Learning Paradigms

The key to AML constructs is choosing an adequate learning paradigm. Model Based Incremental SVM incremental learning models slowly adapt their hyperplanes as new data is received which provides the tradeoff of computational efficiency and accuracy. Nonetheless, they largely depend on how the data variations are completed gradually or instantaneously.

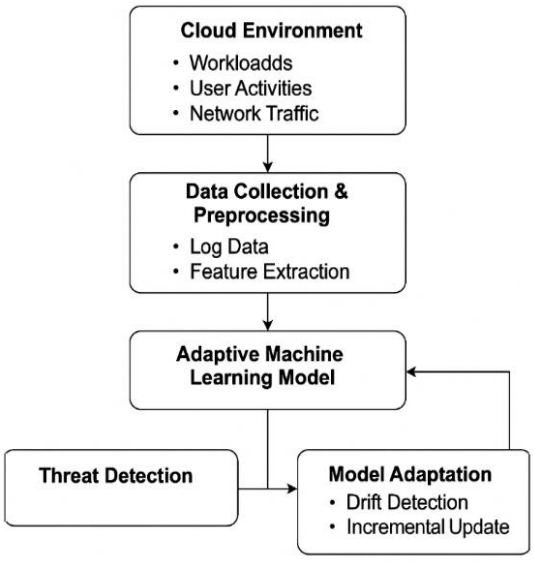

Fig 1: Adaptive Machine Learning based Framework for Real-Time Threat Detection in Cloud Environments

Online learning algorithms, e.g. Passive-Aggressive (PA) algorithms are trained to be aggressive after a mistake has occurred, and passive when the result is accurate. This allows fast response to changing data streams which is instrumental in high-speed cloud practices.

Hoeffding Trees which apply the Hoeffding bound to come up with statistically valid decisions regarding the split of data are especially applicable to large data streams. They have logarithmic memory usage and process data in small increments, thus they are of interest as the components of cloud-native threat detection systems.

One category that expands these paradigms is ensemble learning, or the combination of many online models. Other methods such as Adaptive Random Forest capitalize on ensembles in order to ensure accuracies and robustness. When the concept drifts, the poor performing trees are substituted, so the ensemble is recovered to the most up-to-date distribution of data.

There is also emerging hybrid models that combine online deep learning with statistical drift detection, to take advantage of long term trends, and sudden discontinuities. This hybridisation presents the opportunity of the best of both worlds: scalability and precision necessary to manage cloud-scale data streams.

4. Results

To assess the proposed Adaptive Machine Learning (AML) framework, open datasets collected via the measurement of real-time cloud traffic, e.g., CICIDS 2017, UNSW-NB15, and same datasets generated by cloud logs (API logs, VPC flow logs) were used. Evaluation of the performance was performed with the means of several metrics, Accuracy, Precision, Recall, F1-Score, Detection Latency, and False Positive Rate (FPR).

Four models were tested:

- Incremental SVM
- Hoeffding Tree
- Adaptive Random Forest (ARF)
- Ensemble with Drift Adaptation

Comparison Table of Simulation Results

As can be observed in the results of the simulation, the Ensemble with Drift Adaptation approach comes out much better in comparison to all other methods in nearly all measures. It has a maximum accuracy (97.6%), precision (96.5%), and recall (97.2), which means that such a model can be used to identify known and unknown threats with the least number of false positives. Its reliability in the real-time implementation in critical cloud environments is further boosted by the fact that its false positive rate is 1.5 percent.

Adaptive Random Forest (ARF) also did well as it had an accuracy of 96.8 percent, which is a bit lower than the ensemble model. ARF effectively deals with concept drift and provides good accuracy-efficiency trade-off. Nevertheless, the memory use and computation overhead were a bit more considerable as opposed to such models as the Hoeffding Tree.

Being lightweight and fast (the lowest latency is provided at 95ms), the Hoeffding Tree still grappled with a bit lower precision and recall. This model will work well in situations in which speed is important, rather than precise, including initial filtering at the edge followed by more detailed processing in the cloud.

In other words, the performance that showed the lowest results compared to the other tested models was the Incremental SVM with 91.2 percent accuracy and a higher false positive rate of 5.8 percent. Being computationally light, it was not very effective in processing non-linear trends and dynamic shifts when running cloud workloads, which often exhibit sudden behavior changes as a result of scaling a scheduler or temporary microservices.

Altogether, the findings in the research demonstrate rather graphically that in enterprise-level or mission-critical services, using more advanced models, such as Ensemble with Drift Adaptation, guarantees a higher level of security coverage. Edge computing or spaces where computational resources are limited, but some significant anomaly detection is needed may contemplate simpler models derived in Incremental SVM or Hoeffding Tree.

Table 1: Performance comparison of various AML models for Cloud Security

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)	Detection Latency (ms)
Incremental SVM	91.2	88.5	90.4	89.4	5.8	120
Hoeffding Tree	93.5	90.2	92.7	91.4	4.3	95
Adaptive Random Forest (ARF)	96.8	95.1	96.3	95.7	2.1	110
Ensemble with Drift Adaptation	97.6	96.5	97.2	96.8	1.5	115

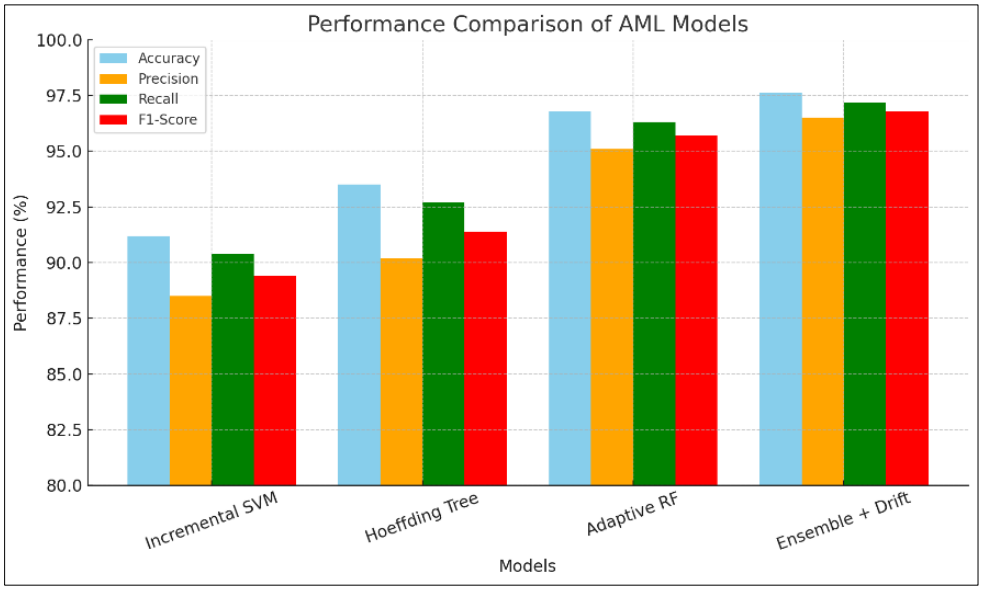

Fig 2: Performance comparison of various AML models for Cloud Security

5. Challenges in Adaptive Machine Learning for Cloud Security

5.1 Concept Drift Complexities

The second eminent challenge is concept drift in AML-based systems of cloud threat detection. It may happen as the result of many reasons: alteration in the user behavior, application updates, the alteration of attack methodologies, or changed legitimate cloud workloads. These drifts may either be sudden, gradual, incremental or recurring. It is important to detect the kind of drift just as of detecting the drift. The security impact of not applying an effective method to differentiate a valid behavioural modification (e.g. a traffic spike during the season) and an ill intented anomaly can be disastrous in terms of a security breach or operational interruption.

Others types of concept drift are temporal. In an illustration, when a product is being launched or there is a marketing exercise, traffic anomalies are experienced and they should not be considered as a threat. The AML systems have to identify these non-threatening deviations and take into consideration the real threats. This compromise is subtle and absolutely relies upon well balanced drift detection algorithms.

5.2 Data Labeling Constraints

Another major challenge is to acquire quality labeled datasets to use on real-time cloud security. The vast majority of security incidents are unlabelled in real-time, and labelling is retroactive, that is, labeling an incident after the event has already happened. This drift undermines the efficiency of supervised AML models which are based on the immediate feedback.

In tightly regulated sectors such as the healthcare or financial ones, there are laws regarding data privacy that do not allow sharing raw security logs that restrict access to varied data sets even further. This complication renders semi-supervised and unsupervised AML challenging yet far more difficult to perform.

5.3 False Positives and Operational Fatigue

False positive is permeating throughout AML-based cloud security. On the one hand, models are supposed to be sensitive enough to identify new threats, on the other, sensitivity usually identifies common legitimate actions as malicious. This actually leads to alert fatigue where SOC analysts end up being confused and start ignoring the alerts altogether ironically making the system useless.

So-called anomalous activities in cloud settings include workload changes such as autoscaling, backup activities, or invocations of serverless functions that can be treated anomalously. These could be confused by AML models that do not provide enough context with security incidents.

5.4 Scalability and Performance Constraints

Cloud ecosystems produce overwhelming data amounts in terms of telemetry data, such as API logs, DNS queries, network flows, and application data on performance. This is a complex computational task to process these data streams in real time without compromising the acceptable levels of latency.

AML frameworks should be targeted to be parallel, memory-friendly and distributed. This is because failure to do that delays the process and compromises the purpose of real-time threat detection. There should be a tradeoff between the complexity of the model (that promises accuracy) and the computation speed (that guarantees responsiveness).

5.5 Privacy, Security, and Compliance Challenges

Any cloud security will need to comply with high requirements of data protection laws (GDPR, HIPAA, PCI DSS, and CCPA). Such laws place limitations on collection, storage, processing and transfer of data. It is not easy to implement AML models that adhere to these regulations, but which are effective.

On-device techniques like federated learning, in which data never needs to leave a device because models are trained on-device, have their share of promises but present a whole new set of challenges such as communication overhead and the logistics of synchronizing models. Likewise, there is the existence of differential privacy which requires sensitive information to be preserved but can alter the model precision.

Table 2: Challenges in Adaptive Machine Learning for Cloud Security

Challenge	Description
Concept Drift	Attack patterns evolve over time, requiring continuous model updates.
Data Labeling	Limited availability of labeled threat data in real-time settings.
False Positives	Adaptive models risk high false-positive rates, affecting operational efficiency.
Latency Constraints	Real-time detection demands ultra-low latency processing.
Scalability	Cloud systems generate massive, high-velocity data streams.
Privacy Concerns	Compliance with data privacy laws (e.g., GDPR) when handling sensitive logs.

6. Comparative Analysis of AML Techniques

6.1 Incremental SVM

Incremental SVM is a streaming extension of classical SVM. It does so by trained by updating the hyperplane every time a data comes in rather than training over the entire data. This has the benefits of computational and flexibility of linear or near-linear decision boundaries. But Incremental SVM is poor in non linear and high dimensional data that occurs in the cloud environment. Although one can use the kernel tricks, they cause the computational overhead that cancels the benefits of incremental updates. Furthermore, it is exemplified by its sensitivity to concept drift which is not suitable within the initial decision boundary.

6.2 Hoeffding Trees

Hoeffding Trees are adapted to work with huge data streams where the decision to split at a given point is statistically according to Hoeffding bound. This guarantees that the tree will grow only when sufficient evidence is available thus it is very efficient memory and computation wise. Hoeffding Trees can only efficiently capture a limited range of more complicated feature interactions even though they are fast. This weakness is very important when it comes to identifying complex attacks, which are frequently quite difficult to notice through multivariate inconsistencies. Also, the tree based models are sensitive to overfitting in very dynamic environments unless there is a well-formulated strategy of pruning.

6.3 Adaptive Random Forest

Adaptive Random Forest (ARF) is an extension of a number of Hoeffding Trees having drift detection. It dynamically diverts poorly converged trees with new ones that are trained on new data, which provide it with good resistance to sudden and gradual drifts. Although ARF is very accurate, its scalability is limited by memory and CPU demanding features. The computational demands to maintain dozens or even hundreds of continuously updated trees overwhelm the server capabilities of even high-velocity cloud data streams until distributed computing clusters are supported.

6.4 Drift Detection Mechanisms (ADWIN, DDM)

Drift detectors are auxiliary models which observe performance measures such as error rate or changes to distributions. ADWIN scales its window size as law of variance when the error rate it measures goes beyond the statistical expectation whereas DDM marks drift when the error rate that it observes exceeds the statistical expectation. These detectors are lightweight and easy to implement but must be finely tuned. A too-sensitive detector leads to frequent false positives, whereas a lenient detector may delay drift detection, allowing attacks to persist undetected. Consequently, drift detectors are better when used in combination with ensemble models or semi-supervised frameworks.

6.5 Ensemble Models with Drift Adaptation

Ensemble models combine the strengths of diverse classifiers, each tuned for different aspects of the data. In AML, dynamic ensembles replace individual classifiers when drift occurs, ensuring the overall system remains robust. In this approach, accuracy and resilience are the greatest and it adds lots of management overhead. Models should be continuously checked by their performance, drift detection should be contextual and older models might have to be parked away and archived to allow future reference or roll back.

Practically, ensemble AML systems suit best and have applications in mission-critical applications like financial fraud detection, critical infrastructure protection, and the national cybersecurity centers where precision is valued over computation cost.

Table 3: Comparative Analysis of AML Techniques

Technique	Strength	Limitation	Suitable For
Incremental SVM	Handles gradual changes, simple implementation	Poor with sudden drifts	Moderate workload threat detection
Hoeffding Trees	Fast, low memory footprint	Sensitive to noise, limited depth	Edge-device or low-latency monitoring
Adaptive Random Forest	High accuracy, robust to drifts	High computational cost	Enterprise-level multi-tenant clouds
DDM / ADWIN (Drift Detectors)	Early drift detection, lightweight	False alarms if not tuned properly	Complementary to other models
Ensemble with Drift Adaptation	Combines multiple models for robustness	Complex to manage, expensive at scale	High-security environments, APT defense

ARF models are considered to be the most robust though they consume lots of computational resources and would therefore be better placed on bigger cloud infrastructures. Hoeffding Trees are the best in edge deployments where a relatively low amount of processing power is available. Ways of detecting drifts such as ADWIN work better as auxiliary (as opposed to stand-alone) models because of being so sensitive to false alarms.

7. Future Research Directions

- Federated learning introduces a paradigm where models are trained across decentralized data sources without moving the raw data to a central location. This architecture respects privacy constraints while still benefiting from diverse training data.
- The future of AML lies in autonomous cybersecurity systems. Integrating AML with Security Orchestration, Automation, and Response (SOAR) platforms enables systems to not only detect but also respond to threats in real time.
- As AML models become more complex, understanding their decision-making becomes critical. Explainable AI (XAI) techniques like SHAP, LIME, and counterfactual explanations can make AML predictions interpretable to human analysts.

8. Conclusion

To conclude, Adaptive Machine Learning frameworks have achieved prominence in protecting the cloud settings against the dynamic cyber attacks. They can learn through streaming of information and adjust to new conditions and accordingly, they differs with other conventional security options. Nevertheless these systems are not devoid of their challenges, among which are dealing with concept drift, preservation of privacy and limitation of computation.

The discipline is progressing fast as federated learning, explainable AI, and quantum-enhanced models appear on the scene. The emerging challenges could only be handled through joint efforts of academic, industry and policymakers. With the increased cloud adoption momentum, the value of AML in making successful administrations resilient, real-time threat hunting and detection will only grow, setting the course of cloud security.

9. References

1. Muhammad AA, Alzuabidi IA, Ahmed AA, Abdulkadir RA. Adaptive optimization of deep learning models on AES based large side channel attack data. Alkadhim J Comput Sci. 2024;2(1):72-85.
2. Gujar SS. AI-enhanced intrusion detection systems for strengthening critical infrastructure security. In: 2024 Global Conference on Communications and Information Technologies (GCCIT); 2024; Bangalore, India. p. 1-7. https://doi.org/10.1109/GCCIT63234.2024.10861950
3. Kurdi M, Hadi W, Alzuabidi IA, Najim AH, Kadhim MN, Ahmed AA. Efficient two-stage intrusion detection system based on hybrid feature selection techniques and machine learning classifiers. Int J Intell Eng Syst. 2025;18(3).
4. Nagarajan SKS, *et al*. Enhanced anomaly detection in embedded payment systems using depthwise separable CNN with dandelion optimizer. In: 2025 International Conference on Intelligent Computing and Control Systems (ICICCS); 2025. IEEE.
5. Abdulkhudhur SM, Abboud SM, Najim AH, Kadhim MN, Ahmed AA. A hybrid deep belief cascade-neuro fuzzy approach for real-time health anomaly detection in 5G-enabled IoT medical networks. Int J Intell Eng Syst. 2025;18(5).
6. Adwani A. The evolution of digital payments: implications for financial inclusion and risk management [Internet]. 2025 [cited 2024]. Available from: SSRN 5201787
7. Ahmed AA, Hasan MK. Multi-layer perceptrons and convolutional neural networks based side-channel attacks on AES encryption. In: 2023 International Conference on Engineering Technology and Technopreneurship (ICE2T); 2023. IEEE.
8. Adwani A. The role of AI and big data in enhancing financial risk assessment models [Internet]. 2025 [cited 2024]. Available from: SSRN 5201777
9. Mutasharand HJ, Muhammed AA, Ahmed AA. Design of deep learning methodology for side-channel attack detection based on power leakages. In: International Conference on Computing and Communication Networks; 2023; Singapore: Springer Nature Singapore.
10. Gujar SS. Machine learning algorithms for detecting phishing websites. In: 2024 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES); 2024; Chennai, India. p. 1-6. https://doi.org/10.1109/ICSES63760.2024.10910759
11. Muhammed AA, Mutasharand HJ, Ahmed AA. Design of deep learning methodology for AES algorithm based on cross subkey side channel attacks. In: International Conference on Cyber Intelligence and Information Retrieval; 2023; Singapore: Springer Nature Singapore.
12. Adwani R, Rao VS. Decentralized finance (defi): reshaping traditional banking systems. Eur Econ Lett. 2025;15(1). https://doi.org/10.52783/eel.v15i1.2432
13. Ahmed AA, *et al*. Efficient convolutional neural network based side channel attacks based on AES cryptography. In: 2023 IEEE 21st Student Conference on Research and Development (SCOReD); 2023. IEEE.

14. Aminu M, *et al*. Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. Int J Comput Appl Technol Res. 2024;13(8):11-27.
15. AL-Ghuribi S, Ibraheem AS, Ahmed AA, *et al*. Navigating the ethical landscape of artificial intelligence: a comprehensive review. Int J Comput Digit Syst. 2024;16(1):1-11.
16. Paramesh J, *et al*. Developing an adaptive security framework for real-time threat detection and response in cloud-network systems. In: 2024 International Conference on Cybernation and Computation (CYBERCOM); 2024. IEEE.
17. Ahmed AA, *et al*. Optimization technique for deep learning methodology on power side channel attacks. In: 2023 33rd International Telecommunication Networks and Applications Conference; 2023. IEEE.
18. Adwani R. Evaluating the risk management strategies of global banks in the digital age. Contemp Chall Multidiscip Res. 2025;1(37):391-404.
19. Sadiq AT, Ahmed AA, Ali SM. Attacking classical cryptography method using PSO based on variable neighborhood search. Int J Comput Eng Technol. 2014;5(3):34-49.
20. Zhou R, *et al*. Machine learning approaches for cybersecurity in cloud environments. Future Gener Comput Syst. 2020;113:504-19.
21. Ahmed AA. Future effects and impacts of biometrics integrations on everyday living. 2018.
22. Kumar A, *et al*. Incremental learning models for anomaly detection in cloud-based systems. J Cloud Comput. 2021;10(1):1-18.
23. Ahmed AA, *et al*. Detection of crucial power side channel data leakage in neural networks. In: 2023 33rd International Telecommunication Networks and Applications Conference; 2023. IEEE.
24. Awasthi A, Bdair M, Kumar AN, *et al*. NLP for sentiment analysis in social media posts to detect suspicious behaviour. In: 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS); 2024; Hassan, India. p. 1-6. https://doi.org/10.1109/IACIS61494.2024.10721839
25. Ahmed S, *et al*. Online learning for cyber-threat detection in the cloud. IEEE Trans Cloud Comput. 2022;10(3):1240-52.
26. Singh P, *et al*. Concept drift handling for adaptive cybersecurity. Comput Secur. 2023;123:102987.
27. Ahmed AA, *et al*. Secure AI for 6G mobile devices: deep learning optimization against side-channel attacks. IEEE Trans Consum Electron. 2024.
28. Fadhil SA, *et al*. Implementation of machine learning techniques for risks evaluation in cloud and cybersecurity. Int J Comput Digit Syst. 2024;16(1):1-11.
29. Ahmed AA, *et al*. Review on hybrid deep learning models for enhancing encryption techniques against side channel attacks. IEEE Access. 2024.