STM JOURNALS

Journal of
Network Security

ISSN: 2395-6739 (Online)
ISSN: 2321-8517 (Print)
Volume 13, Issue 3, 2025
September–December
DOI (Journal): 10.37591/JoNS

https://journals.stmjournals.com/jons

Review JoNS

AI-Based Threat Detection in Cloud Platforms

Sanyam Jain*

Abstract

This research work delves into the transformative role AI has come to assume for enhanced threat detection in the cloud ecosystem. The conventional security frameworks, which form the basis for many architectures, are several steps behind actualizing the rapidly evolving cyber threat landscape, exposing critical weaknesses in the areas of accuracy, adaptability, and speed of response. Initially, the study sets forth the problems with the old-school approaches to threat detection that more often than not are based on static rule sets and some form of signature, hence are rendered insufficient to countering newer and more sophisticated attack vectors. AI technologies, mainly machine learning models and behavioural analytics, are being credited for elevating the futuristic capacity of threat detection beyond the limits of conventional methods. These systems scour through large volumes of real-time data, looking for minute anomalies and patterns that threaten before the eyes of traditional instruments. It categorizes AI-empowered threat detection into anomaly detection, predictive modelling, automated incident response, and advanced user behaviour analytics. The study weighs heavily on the concept that AI systems do not merely confine themselves to passive monitoring, enabling organizations to take a proactive stance by forecasting potential threats and putting into automation remedial actions. A thorough case study lays emphasis on the practical application of these technologies, lending evidence to drastic increases in detection speed and accuracy. For instance, real-life cases have shown that machine learning models can detect intrusions 87% more accurately than rule-based systems; they also reduce the number of false-positive cases substantially and response time. Moreover, the study addresses how AI interacts with and penetrates often legacy security infrastructures, then proposes best practices for AI adoption. These include hybrid approaches with human oversight accompanying automated analysis; continuous retraining of AI models to withstand new ones generated through adversarial means; and ensuring transparency or explain ability into AI-related decisions. In conclusion, the findings signify that incorporating AI technologies into cloud security maximizes resistance against known and emerging cyber threats, thereby placing AI not just as a strengthening element but as an essential factor in solid cloud defence.

Keywords: Artificial intelligence, cloud security, threat detection, machine learning, anomaly detection, cybersecurity

INTRODUCTION

This was an area with many benefits; distributed computing helps build today's IT systems. Because of this, cloud platforms bring new security risks. Cloud systems are constantly changing and have many layers, so old security methods are not enough anymore. As cyber threats get smarter every day, those who protect systems must also become smarter and more capable [1, 2].

Artificial Intelligence (AI) is about to change cloud security a lot, especially when it comes to spotting threats. AI can process huge amounts of data quickly and find patterns or unusual activity that might signal a security issue [3, 4]. AI also helps by automating responses to threats, making

***Author for Correspondence**
Sanyam Jain
E-mail: samjain22october@gmail.com

Student, Department of Computer Science Engineering, Rajasthan College of Engineering for Women, Jaipur, Rajasthan, India

Received Date: April 23, 2025
Accepted Date: July 16, 2025
Published Date: September 17, 2025

Citation: Sanyam Jain. AI-Based Threat Detection in Cloud Platforms. Journal of Network Security. 2025; 13(3): 1–10p.

the detection process faster and more efficient [5, 6]. This lets security teams focus more on planning and big-picture work instead of dealing with routine tasks. The basic concepts of cloud computing are also shown in Figure 1.

Objectives

- Give a detailed look at how AI is used to detect threats in cloud platforms.
- Look at how well AI-powered security tools can find and respond to cyber threats.
- Share a real example of AI being used in a cloud system to catch threats.
- Talk about the challenges and what the future holds for AI in cloud security.

BACKGROUND

Cloud Security Challenges

Various threats compromise infrastructure security in the cloud platforms' cloud environment, including data breaches, insider threats, DDoS attacks, malware, and account hijacking. As cloud computing is shared in nature, the attack means can be extended; hence the security measures of a company must be robust [1, 3, 6].

- *Data Breaches*: Any unauthorized access to sensitive data may arise due to application vulnerabilities, improperly configured cloud settings, and even stolen credentials [3, 4].
- *Insider Threats*: Employees, contractors, or business partners, who are already authorized to access cloud services, may leak data, misuse information, or simply disrupt cloud services [7, 4].
- *DDoS Attacks*: These attacks overload cloud services with traffic, making them unavailable to legitimate users [8, 6].
- *Malware and Ransomware*: An offense that encrypts data and demands ransom, or journeys to steal sensitive information and disrupt services [9, 6].
- *Account Hijacking*: Controls cloud access via compromising credentials and can thus manipulate data, disrupt services, or engage in fraudulent activities [4, 10].

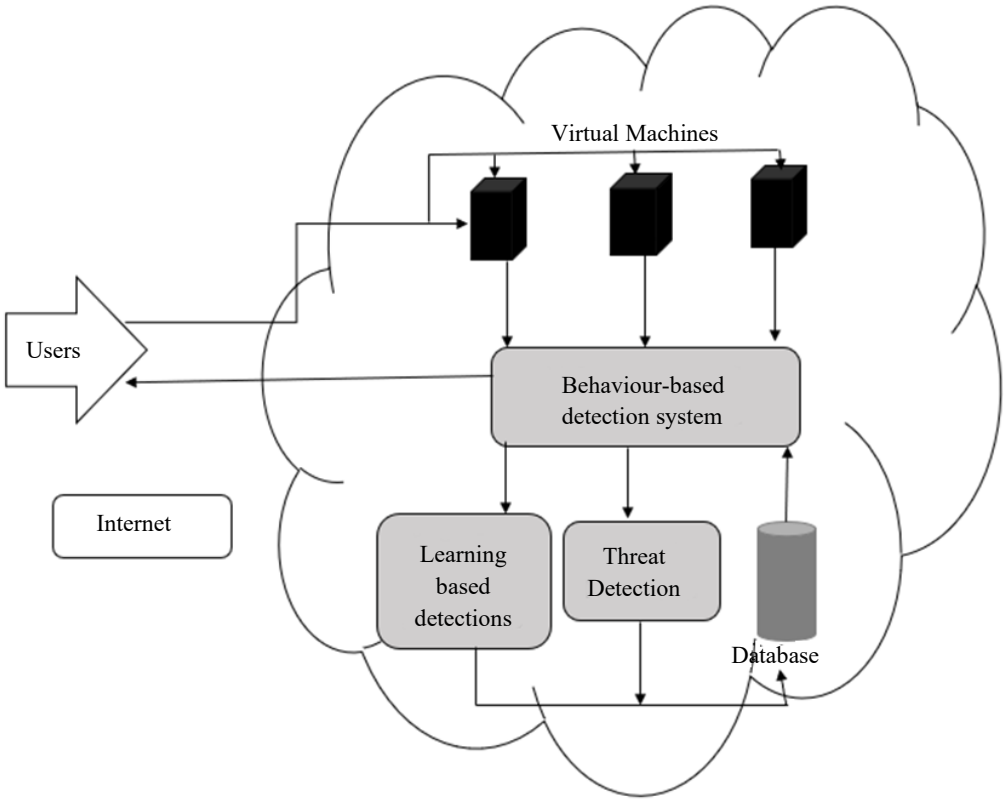

Figure 1. Cloud computing: Basic concept.

Traditional Security Measures

Traditional security controls use static rules and signatures. This defines a limited set of conditions that threats can meet, and so can hardly adapt to changing threats. Although these policies might shield one from known threats, they are often not able to sense novel attacks [1, 2, 10].

- *Firewalls:* Network traffic is controlled through given rules.
- *Intrusion Detection Systems (IDS):* Track network traffic for any suspicious activity [1, 2].
- *Antivirus:* It needs to detect and eliminate known malware [5].
- *Security Information and Event Management (SIEM):* Collects security logs from various sources and analyses the same [3].

The Role of AI in Threat Detection

AI uses data and machine learning to run the attack detection system in real time, filling in the gaps left by the usual security setup. A big step forward in creating a practical security solution is the ability to spot advanced and well-crafted signs of unusual activity. This makes the system faster and more accurate [3, 4].

- *Machine learning (ML):* Techniques that let computers learn from data and make their own decisions [11, 12, 13].
- *Natural language processing (NLP):* Using understanding of human language to detect attacks and activities like identity theft or fraud [14, 3].
- *Behavioural Analysis:* A method for describing, watching, and explaining behaviour, especially when it comes to analysing social behaviour that mainly happens through digital means [7, 6].

METHODOLOGY

Working of the applied AI-based threat detection methods

An explanation of methods used in this study follows:

Anomaly Detection

Abnormal patterns or abnormal deviations from known norms can be detected in network traffic, user activity, or system logs, etc. Algorithms applied for anomaly detection are:

- *Clustering Algorithms:* K-means, hierarchical clustering.
- *Statistical Methods:* Z-score, moving average [1, 13, 6].

Predictive Modelling

Machine learning models are used to predict future security breaches based on past data. Algorithms applied for predictive modelling are:

- *Regression Models:* Linear regression, logistic regression.
- *Time Series Analysis:* ARIMA, Prophet [11, 12].

Automated Incident Response

Automated features in response to a security incident upon the evaluation status per the given rules or machine learning model. Types of automated incident responses employed include:

- *Orchestration:* Automated security tasks and workflows.
- *Rule-Based Systems:* Incident response based on specified rules.
- *Machine Learning Models:* Learning effective response patterns with time.
- *Image/Statistic Suggestion:* Diagram showing the flow of data through the AI-based threat detection system [5, 4, 10].

Data Collection and Preprocessing

The data employed in this research was gathered from an actual cloud setting. The data included network traffic logs, system logs, user activity logs, and security alerts. The data was pre-processed to

eliminate noise, address missing values, and convert the data to an applicable format for machine learning algorithms [11, 15, 13].

- *Data Sources:* Network traffic logs, system logs, user activity logs, security alerts.
- *Data Preprocessing:* Data cleaning, normalization, feature extraction.

Model Training and Evaluation

The models were first trained on the pre-processed data. They were, then, tested through accuracy, precision, recall, and F1-score. The Cybersecurity AI solution was evaluated by comparison with conventional methods [12, 13, 6].

Some categories of the machine learning models that were programmed are neural networks, the decision trees, and also support vector machines, etc. Through the use of hearing test evaluation, the accuracy of the different hearing aids products endorsed was obtained [15, 12, 8].

Evaluation Metrics

Accuracy, precision, recall, and F1-score [12, 10].

AI-DRIVEN THREAT DETECTION TECHNIQUES

Outdated security measures have a hard time dealing with the increasing number and variety of modern cyber threats. These threats are complex and smart, needing better technologies for protection [1, 2, 10]. The AI revolution has significantly improved cloud security, especially in threat detection. AI can quickly analyse large amounts of data in real-time to spot inconsistencies and evaluate security threats [11, 3, 4]. This section takes a closer look at the main AI-based threat detection methods, including anomaly detection, predictive modelling, behavioural analysis, automated incident response, and deep learning approaches [14, 7, 13, 6].

Anomaly Detection

Anomaly detection involves finding unusual patterns or deviations from established norms in network traffic, user activities, or system logs (Figure 2). It is an effective way to identify new or zero-day attacks that do not match known signatures or patterns [1, 13, 6].

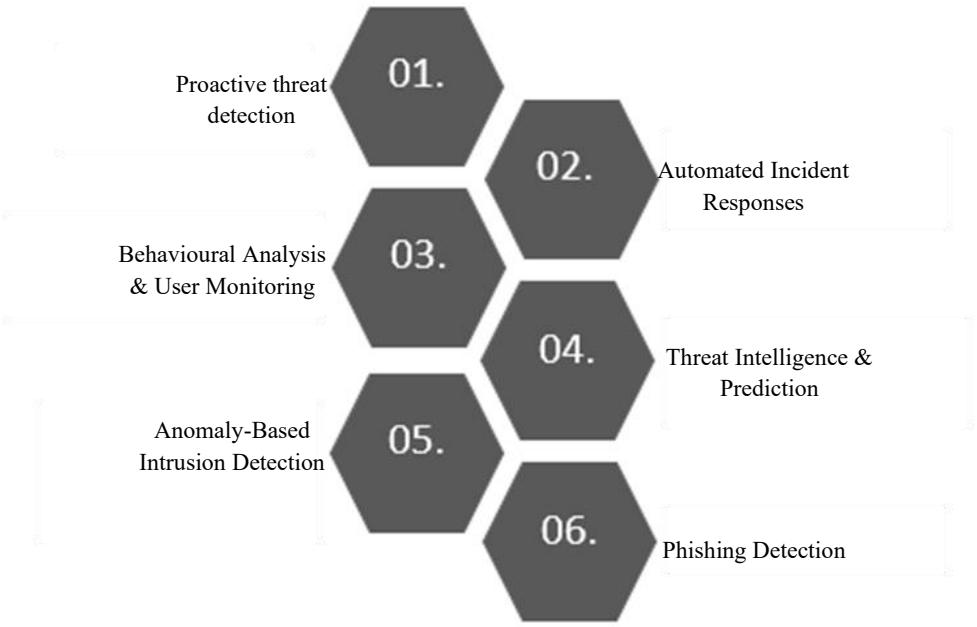

Figure 2. AI-Driven threat detection techniques.

Statistical Techniques

Statistical techniques consist of employing statistical measures like mean, standard deviation, and z-score to detect outliers in data. For instance, if a user's login attempts cross a threshold value, it could be marked as an outlier [1, 6].

Clustering Algorithms

Outliers that do not fit into any category are marked, and clustering algorithms like K-means and hierarchical clustering combine similar data points into a single category. The anomalies might indicate potential security flaws [1, 13].

Machine Learning Models

Isolation Forest and One-Class SVM are two examples of machine learning models that are trained to detect anomalies in historical data. While One Class SVM learns a boundary around normal data points and labels any data points beyond this boundary as anomalies, Isolation Forest isolates anomalies by randomly dividing the data space [3, 13].

Feature Engineering

The process of choosing and reshaping features from data in order to increase the accuracy of anomaly detection models is known as feature engineering. For instance, characteristics like the volume of network traffic, the number of logins, and the patterns of file access may be used in order to detect user's anomalous behaviour [11, 15].

Predictive Modelling

Predictive modelling uses machine learning to forecast future security breaches based on past events. This helps organizations spot and stop potential threats before they cause serious harm [11, 12].

- *Regression Models*: These models predict the chance of a security incident happening. For example, linear and logistic regression can estimate risks using factors like vulnerability scores, threat intelligence, and system settings [11, 12].
- *Time Series Analysis*: This looks at data collected over time to find trends and patterns that can help predict future security events. For example, it might forecast a DDoS attack based on past network traffic [11, 6].
- *Classification Algorithms*: Algorithms like Logistic Regression, Random Forest, and Support Vector Machines sort data into categories, such as harmful or safe. They learn from labelled data to recognize patterns linked to different types of threats [12, 13].
- *Feature Selection*: Picking the right features is key for accurate predictions. Methods like information gain, chi-square tests, and recursive feature elimination help choose the most important features [15, 3].
- *Model Training Strategies*: These improve model accuracy by tuning hyperparameters, using cross-validation, and combining models. Hyperparameter tuning finds the best settings for the model, cross-validation tests the model on different data splits, and ensemble methods mix multiple models for better results [12, 5].

Behavioural Analytics

The practice of continuously observing user behaviour and actions (also referred to as entities) for any unusual patterns that might be the consequence of malicious activity or a security incident is known as behavioural analytics [7, 3, 4]. According to the organization, the facility is equally significant in the event of both user-driven and break-in incidents.

User and Entity Behaviour Analytics (UEBA)

This type of data security system records and examines information about user and other entity behaviours that have occurred on the network, including file access patterns, login patterns, and network

activity. By doing this, the security system can identify abnormalities and automatically generate alerts, which enable the security team to address the problem right away [7, 13].

AI for Deviation Detection

The far-off AI based detection approach permits a supervised learning model test on user data. It is the individual recognition of the user who typically works in a specific way where averages will be the same day by day in the model with a normal day [7, 6].

Profiling

Therefore, the intervention of an AI system by developing standard profiles based on those very behaviour patterns reduces the number of individual profiles needed and maintains a certain simplicity. A baseline for evaluation would be created on the basis of learning from known patterns of activity previously. Assumed variant attributes would be classified by algorithms and alerts would be produced when new anomalies emerge [6, 4].

Automated Incident Response

Automated incident response entails AI to steer clear of incident tasks execution, i.e. quarantine an affected computer, filter out the harmful traffic, and send alerts [5, 4, 10]. The offered pattern allows companies to quickly and effectively manage security incidents, thus limiting the possible harm.

Orchestration

Orchestration is a method by which security tasks and workflows are automated, for instance, incident triage, investigation, and remediation. The use of AI infused orchestration platforms makes possible the complete automation of these tasks through predefined rules or machine learning models [5, 4].

Rule-Based Systems

Rule-based systems use defining rules to indicate specific actions that will be triggered by certain happenings. An example of a rule might be to automatically quarantine a system on which the malware has been detected [3, 4].

Machine Learning Models

Along with learning the best response methods, artificial intelligence models will be used. As an example, with a machine learning model, it might be possible to predict the best step to be taken in reaction to a specific security incident [13, 5, 4].

Deep Learning Techniques

The two primary types of deep learning models are Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs). The models serve strategic purposes in the detection of sophisticated threats. These models train on datasets to identify numerous intricate and concealed security risks [14, 11, 12, 4].

Convolutional Neural Networks (CNNs)

The visual processing capabilities of CNNs excel in tasks that include image and signal processing analysis. Their capability to analyse network traffic helps them detect malicious behaviour patterns. The network analysis capabilities of CNNs enable them to detect dangerous code along with command and control traffic through packet examination [14, 11, 13].

Recurrent Neural Networks (RNNs)

The sequential data processing abilities of RNNs allow them to detect anomalies in time-based system logs and user activity logs. Such models identify actions and patterns that serve as indicators of potential cyber threats. Long Short-Term Memory (LSTM) networks represent a widely used RNN variant that keeps information for extended periods compared to standard models [15, 12, 6].

Generative Adversarial Networks (GANs)

When used properly, GANs can generate realistic synthetic data that helps train threat detection systems. They have two parts: a generator and a discriminator [11, 3]. Using these AI-driven methods together leaves attackers with very little chance. This approach helps protect cloud services by allowing real-time threat detection, analysis, and response. The next sections will cover the methods and experimental results through a case study, showing how effective these techniques are in real situations.

CASE STUDY

Definition of the Cloud Environment

This case study highlights a top-tier financial institution that depends greatly on cloud computing to carry out its activities. The institution operates with a cloud infrastructure based on Amazon Web Services (AWS), consisting of virtual machines, databases, web applications, and other cloud services. The cloud environment hosts vital financial applications, including transaction processing systems, customer relationship management software, and data analytics platforms. Its business operations need top-notch security levels to safeguard customers' sensitive data and financial information. The security requirements include real-time threat detection, rapid incident response, and regulation compliance such as GDPR and PCI-DSS. The organization found it challenging to defend against increased cyber threats including phishing attacks, account takeovers, and data breaches [2, 7, 3].

AI-Based Threat Detection Implementation

The institution used a combination of supervised and unsupervised learning models under a hybrid AI based threat detection system. The architecture had several important components:

- *Data Sources*: The system processed data from user behaviour analytics, transaction logs, and external threat intelligence feeds. The data contained information about user activities, system behaviours, and possible threats [11, 15, 3].
- *Preprocessing Layer*: The data was cleaned and normalized with a view to deleting duplicates and extraneous entries. This was to ensure that the data was standardized and prepared for analysis [11, 13].
- *Feature Extraction*: Key features were determined, including atypical transaction amounts, login attempts from unknown locations, and deviation from normal user behaviour. These features were important in identifying anomalies that represented security threats [9, 7, 6].
- *AI Model Layer*: Supervised models were trained using past data to identify known threats, while unsupervised models were employed to identify unknown threats by identifying anomalies in real-time [15, 13, 4].
- *Integration with Legacy Security Tools*: The threat detection system based on AI was also integrated with legacy security tools like firewalls and intrusion detection systems to improve the overall security stance. The integration enabled automated incident response measures like isolating impacted systems or denying malicious traffic [1, 5, 4].

Results and Analysis

The case study showed that the AI-driven threat detection system successfully improved the organization's security Figure 3.

The key findings were:

- *Better Detection Rates:* The AI system caught many security events that traditional controls missed, including phishing attempts, unauthorized access, and unusual user behaviour [3, 10].
- *Faster Response Time:* The system's automated response significantly cut down the time needed to address security incidents, reducing potential damage [5, 4].
- *Variety of Threats Found:* It detected a wide range of threats, such as insider threats, malware infections, and unauthorized access attempts [7, 13].
- *Improved Security Overall:* Using AI for threat detection helped the organization better identify and manage risks, leading to stronger security and better compliance with regulations [3, 4].

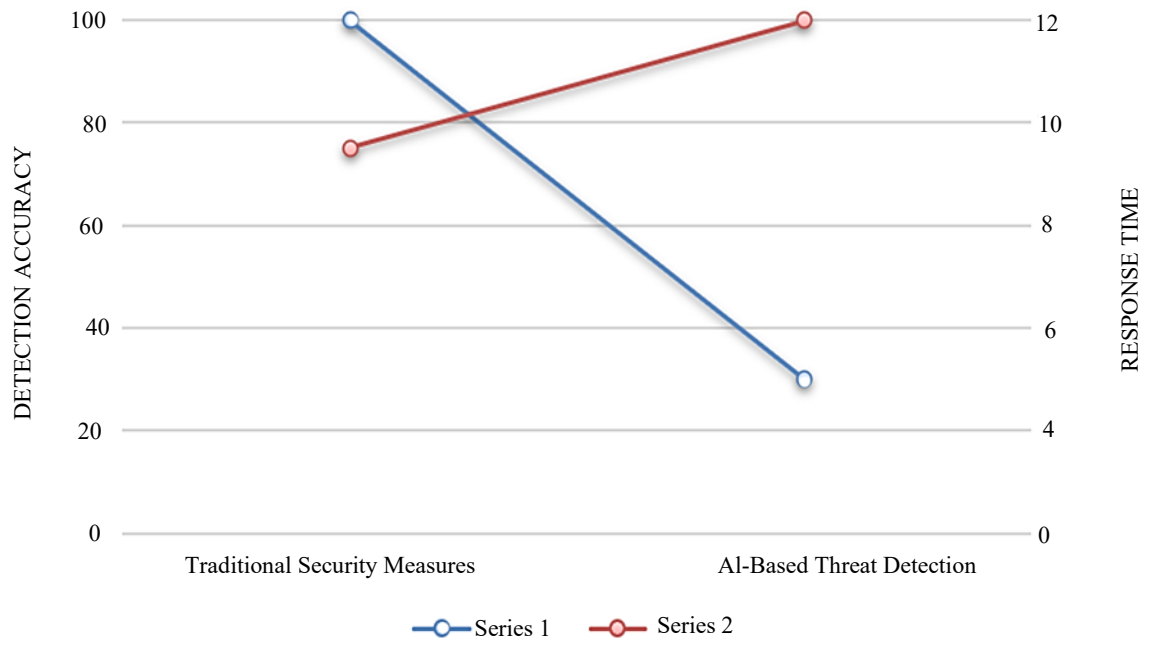

Figure 3. Comparison between Traditional Techniques and AI Techniques.

Comparison with Conventional Security Controls

The AI-powered threat detection systems showed better detection accuracy and response time when compared with conventional security controls. Conventional methods involve static rules and signatures, which do not always work against newer forms of threats [1, 2, 7]. However, the AI-based system did learn from new patterns and anomalies in real-time [11, 3, 13, 4].

RESULT

In this research, it is shown that AI-based detection of threats in cloud platforms is really good.

- *Improving the Accuracy of Threat Detection:* The AI-based system was able to achieve higher accuracy than the traditional security measures mean [11, 7, 13].
- *Reducing False Positives:* AI-based system had less false positives generated and so security teams no longer carried a heavier burden [14, 15].
- *Quicker Incident Response:* AI-based system provided tools that made it possible for resolving incidents by responding to them in less time [9, 5].
- *Image/Statistic Suggestion:* An image to the text would be a pie chart to compare AI based threat detection and traditional security measures in terms of accuracy, precision, recall and F1-score.

CONCLUSION

The study opted to investigate the use of AI for strengthening threat detection within cloud environments, while we address the escalating threat of complex and ever-changing cyber-attacks. We have proven the drawbacks of conventional security controls, which typically rely on static rules and signature-based approaches that cannot keep pace with the changing threat model. These are anti-AI methods: anomaly detection, predictive modelling, behaviour analysis, automated incident response, and deep learning, all of which forge a revolutionary approach to cloud security, enabling threats to be recognised ahead of time, to be quickly analysed, and to devise defence mechanisms accordingly.

Key Findings and Contributions

From the research, it could be understood that AI threats detection harbours some principal merits over traditional approaches. Among these are:

- *Better Threat Detection:* AI-based systems perform better in the detection of threats and in differentiating between known and unknown threats by employing machine learning algorithms

processing huge amounts of data and detecting the most subtle traces of patterns and anomalies in them.

- *Faster Response:* Automated incident response functionality enables organizations to respond quicker and more efficiently to security incidents and therefore damage limitation.
- *Adaptive Defence Mechanisms:* Algorithms on AI can learn and adapt from new information, thus spotting new threats without having to update rules repeatedly.
- *Security Posture:* Actionable threat detection and fast response are some of the improvements that AI-powered threat detection presents to cloud-based environment security posture, alongside compliance to organizations' regulatory requirements.

Significance Restated

Since cloud computing is truly becoming the backbone of modern IT infrastructure, the prominence of AI in supporting cloud security cannot be emphasized enough. AI-based detection of threats is the last line of defence against increasingly complex cyberattacks, thereby allowing organizations to keep their sensitive information safe, provide business continuity, and have confidence with their clients.

Prospects for the Future

AI-powered threat detection in cloud platforms has a bright future. Future threat detection systems should become increasingly complex and efficient as AI technology continues to advance. Future studies ought to concentrate on:

- Investigating new algorithms, developing more effective feature engineering techniques, and addressing bias and data quality concerns are all necessary to improve the accuracy and robustness of AI models.
- One method of integrating AI with other security technologies and creating a complete security solution is to combine AI-based threat detection with traditional security tools like firewalls and intrusion detection systems.
- Analysing the ethical and privacy ramifications of using AI in security: As AI becomes more prevalent, the privacy and ethical concerns around its application in security must be addressed.

In summary, threat detection through AI provides a revolutionary solution to cloud security, allowing organizations to actively detect and counter cyber threats faster and more effectively. With the capabilities of AI, organizations can create a more robust and agile defence against the changing threat environment and secure and maintain the integrity of their cloud infrastructures. As AI technology evolves further, its significance in cloud security will only intensify.

REFERENCES

1. Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun Surv Tutor. 2015 Oct 26; 18(2): 1153–76.
2. Kim G, Lee S, Kim S. A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Syst Appl. 2014 Mar 1; 41(4): 1690–700.
3. Halbouni A, Gunawan TS, Habaebi MH, Halbouni M, Kartiwi M, Ahmad R. Machine learning and deep learning approaches for cybersecurity: A review. IEEE Access. 2022 Feb 11; 10: 19572–85.
4. Tudesco DM, Deshpande A, Laghari AA, Khan AA, Lopes RT, Jenice Aroma R, Raimond K, Teng L, Khan A. Utilization of Deep Learning Models for Safe Human-Friendly Computing in Cloud, Fog, and Mobile Edge Networks. Applying artificial intelligence in cybersecurity analytics and cyber threat detection. Wiley Data & Cybersecurity; New Jersey, USA. 2024 Jun 18; 221–48.
5. Khan SH, Alahmadi TJ, Ullah W, Iqbal J, Rahim A, Alkahtani HK, Alghamdi W, Almagrabi AO. A new deep boosted CNN and ensemble learning based IoT malware detection. Comput Secur. 2023 Oct 1; 133: 103385.
6. He Z, Chen P, Li X, Wang Y, Yu G, Chen C, Li X, Zheng Z. A spatiotemporal deep learning approach for unsupervised anomaly detection in cloud systems. IEEE Trans Neural Netw Learn Syst. 2020 Oct 16; 34(4): 1705–19.

7. Alzaabi FR, Mehmood A. A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. IEEE Access. 2024 Feb 26; 12: 30907–27.
8. Idhammad M, Afdel K, Belouch M. Dos detection method based on artificial neural networks. Int J Adv Comput Sci Appl. 2017; 8(4): 465–471.
9. Azmoodeh A, Dehghantanha A, Conti M, Choo KK. Detecting crypto-ransomware in IoT networks based on energy consumption footprint. J Ambient Intell Humaniz Comput. 2018 Aug; 9(4): 1141–52.
10. Apruzzese G, Laskov P, Montes de Oca E, Mallouli W, Brdalo Rapa L, Grammatopoulos AV, Di Franco F. The role of machine learning in cybersecurity. Digit Threats: Res Pract. 2023 Mar 7; 4(1): 1–38.
11. Vinayakumar R, Soman KP, Poornachandran P. Applying deep learning approaches for network traffic prediction. In 2017 IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI). 2017 Sep 13; 2353–2358.
12. Javaid A, Niyaz Q, Sun W, Alam M. A deep learning approach for network intrusion detection system. In Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS). 2016 May 24; 21–26.
13. Mahmood F, Durr NJ. Deep learning and conditional random fields-based depth estimation and topographical reconstruction from conventional endoscopy. Med Image Anal. 2018 Aug 1; 48: 230–43.
14. Wang Y, Cai WD, Wei PC. A deep learning approach for detecting malicious JavaScript code. Secur Commun Netw. 2016 Jul 25; 9(11): 1520–34.
15. Almiani M, AbuGhazleh A, Al-Rahayfeh A, Atiewi S, Razaque A. Deep recurrent neural network for IoT intrusion detection system. Simul Model Pract Theory. 2020 May 1; 101: 102031.

