ESP-IJACT
ESP International Journal of Advancements in Computational Technology
ISSN: 2583-8628 / Volume 1 Issue 1 June 2023 / Page No: 150-159
Paper Id: IJACT-V1I1P120 / Doi: 10.56472/25838628/IJACT-V1I1P120

Original Article

AI-Powered Cloud Security: A Unified Approach to Threat Modeling and Vulnerability Management

Chaitanya Vootkuri
Distinguished Cloud Security Architect, USA.

Received Date: 19 April 2023 Revised Date: 22 May 2023 Accepted Date: 18 June 2023

Abstract: *Cloud computing has become one of the most important tools that have transformed business by providing solutions at the right price. Huge global popularity has led to the seemingly countless number of cloud services, and thus, security has become a critical issue. The technology known as Artificial Intelligence (AI) has turned out to become a useful weapon to fight against these challenges since threat detection, management of vulnerabilities, limiting threat proneness and formation of counterattacks can be availed through AI solutions. This paper introduces a single model of AI application in cloud security that addresses threat modeling and vulnerability assessment and management. This approach thus improves the dynamism and responsiveness of CS systems by using AI techniques like machine learning, natural language processing and anomaly detection. This paper also analyses how AI is integrated with traditional cloud platforms or architectures, as well as the advantages and disadvantages of doing so. Specific contributions made include a thorough analysis of how AI can be applied to cloud security, an analysis of its effectiveness, and an examination of the development trajectories of AI in clouds. The conclusions presented in the paper clearly demonstrate the ability of AI to radically change the protection of cloud structures from modern cyber threats.*

Keywords: *Cloud Computing, Threat Modeling, Vulnerability Management, Machine Learning, Cybersecurity, Anomaly Detection.*

I. INTRODUCTION

A. Importance of Threat Modeling and Vulnerability Management

Figure 1: Importance of Threat Modeling and Vulnerability Management

a) Understanding Threat Modeling:

Threat modeling is an important best practice to understand the threats rising out of a certain system and how to address them, especially in a cloud setting, given the multiple levels and components in contemporary cloud systems. In essence, threat modeling can reduce the risk of a cyber-attack and inform security teams how to structure the environment and manage data moving within an environment. [1-3] Some of the benefits that organisations derive include: This enables the management to appreciate the risk profile and make an informed decision on what risk to undertake, how to do it, the likelihood and likely impact of the risk, and how to handle or manage such risks. Threat modeling goes beyond merely identifying current threats; it also identifies future threats since the nature of risks changes with time.

b) Prioritising Vulnerabilities for Efficient Remediation:

Vulnerability prioritisation goes beyond simply recognising risks; it aims to rank them to fix major problems as much as possible. Because there can be innumerable amounts of risks inherent in any given cloud structure, it is important to determine which risks are most dangerous to the enterprise. Threat-based analysis methods allow the security team to work on the most important issue at any given time, as identified by threat modelling, rather than tackling all issues simultaneously. It enhances resource utilisation since the core of the problem is addressed, shortens the time required for remedial actions, and greatly enhances security.

c) Reducing the Attack Surface:

Threat modeling and vulnerability management both play a part in diminishing attack surface or attack vector, an aggregate of points of access where unauthorized intrusions can occur. Using threat modeling, the security specialist can filter where the attacker may try to take advantage of the vulnerability, like an unsecured API, open ports or an improperly configured cloud service. After predictions, vulnerability management processes try to address these deficits through code fixes, increased security policies, or varying access control measures. Through this process of iteration on the attack surface, the opportunities available to an attacker to exploit the systems in an organisation's cloud environment are minimised, and in general, the security of the cloud infrastructure is increased.

d) Improving Incident Response and Recovery:

Risk analysis and vulnerability assessments are primary components of the response and planning related to the incidence. These approaches allow security managers to make more sound strategies for approaching the threat factors their systems will likely encounter. Threat models make determining the higher-risk attack scenarios easier so proper defence plans and response procedures can be developed. Risk management ensures that risks are prevented so weaknesses can be exploited. Having a clear picture of what we are protecting and how to protect it helps when there is a breach; identifying complicating factors and developing suggestions of expectation shortens the time to recover from the breach and limits the damage from a security breach.

e) Enhancing Compliance and Risk Management:

Threat modeling and vulnerability management go hand in hand with compliance with industry regulatory bodies and risk management frameworks Compliance. Most current regulation standards like GDPR, HIPAA and PCI-DSS, for instance, demand that organisations periodically evaluate and systematically look for risks and related vulnerabilities in ways that they can also look for appropriate measures to safeguard sensitive information. Threat modeling and vulnerability management practices show that an organisation recognises compliance status and undertakes steps to prevent risk events leading to non-compliance conditions. When assessing and using threats and vulnerabilities within a comprehensive risk approach, an organisation works towards enhanced cloud protection and compliance to prevent penalties and reputational losses from security threats.

B. Role of AI in Cloud Security

Artificial Intelligence (AI) has emerged as a powerful enabler for enhancing cloud security. [4,5] By employing advanced algorithms, AI offers:

Figure 2: Role of AI in Cloud Security

a) Proactive Threat Detection:

AI is, therefore, instrumental in the early detection of threats in cloud security since it is proactive. Most conventional security mechanisms are detection-based, wherein an organisation may not detect new or zero-day attacks, which are novel. AI can detect abnormalities in traffic patterns, user behaviour, and system activities, especially using machine learning and deep learning approaches. Thus, the fact that AI models can identify such patterns of behaviour as abnormal means that threats can be identified much earlier than traditional systems, including those at the zero-day level, which are often not noticed. Because AI

can continuously learn from data, it can identify growing trends of new threats and adapted techniques, bringing a vastly beneficial approach to cloud environments, which are constantly threatened by escalating threat levels.

b) Scalable Security Solutions:

Cloud environments are normally expansive and often heterogeneous and complex, with many large data sets and a number of virtual instances active at any one time. One of the major limitations of conventional security solutions pertains to scalability, the ability to keep up with the volume and density of cloud environments, and the demands they place on safety and security features. AI helps to overcome this problem by providing Network Security Solutions that can expand in pace with large scales and adjust to the load of those large scales. Reducing security orchestration through intelligent automation of monitors, threats, and vulnerability scans, AI can analyse and process vast amounts of data sets in real time and maintain constant security operations across cloud services and infrastructure elements. This scalability cuts down on the workload demands on security teams so they can handle higher-value work and let AI take care of the continuous detection and response tasks.

c) Adaptive Learning:

Quite uniquely, one of the key benefits of AI, when applied to cloud security, is that it can learn. Conventional security measures on networks often depend on set patterns or formats of attacks well known to the analyst or are easily changed after attack detection. On the other hand, AI systems can learn, get updated and modify with time depending on new information, such as a changing threat behaviour pattern or novel attack type. These continual learning methods allow the AI model to learn new threats or identify new attack vectors of a threat, such as a new version of malware or Advanced Persistent Threats, without updating or modifying the rules. Due to their ability to learn from new data, AI technologies are perfect for responding to innovations in cyber threats, guaranteeing that security controls are optimal in combating novelty threats in the continually evolving world.

C. Challenges in Cloud Security

Cloud security is a major problem because of features of contemporary cloud structures that classical security instruments do not address successfully. This, together with the fact that cloud environments can be continuously changing, makes it hard to manage. Cloud solutions are flexible, meaning resources can be quickly and easily provisioned or de-provisioned to meet performance requirements. Though this flexibility is one of the greatest strengths, static security models are insufficient because they cannot promptly respond to environmental changes and thus are full of holes that adversaries will be happy to use. For example, security configurations may lag new instances or services that create a situation in which the probability of exposure rises. The fourth compelling issue is the distributed structure of Cloud systems. Most cloud solutions follow a multi tenant model where many consumers jointly use resources like storage, CPU, memory, etc. This architecture puts additional data leakage threats since data might contain sensitive information about one tenant, and it's easily exposed to other clients if the service provider experiences a vulnerability in their resources. Maintaining proper data segregation and the correct data permissions are critical; however, frequently available tools cannot provide granular and flexible access control for these extensive structures. Moreover, cloud ecosystems are rather complex, making these issues even more difficult to manage. Cloud platforms typically combine heterogeneous technologies, platforms, and APIs, all of which may have different security needs and a different set of risks. Securing such a broad terrain of landscapes requires unified and coordinated admin, which is challenging, with reasonable security management tools still geared towards more routine centralised data storage systems. A lack of proper configurations – often the case in large environments continues to be one of the biggest root causes of cloud security incidents. To overcome these challenges, security solutions must be clever, dynamic and appropriate to cloud environments, requiring auto control features, strong artificial intelligence facilities to detect threats and centralised control to protect the cloud environment.

II. LITERATURE SURVEY

A. Traditional Cloud Security Mechanisms

The classical approach to cloud securing leverages absolutory measures, including firewalls, encryption protocol and intrusion detection systems. A firewall regulates network traffic flow and access, and encryption helps maintain a file's privacy when stored and in transit. At the same time, an IDS identifies a violation or an intrusion by studying network traffic. [6-9] However, these approaches are more based on rules and signatures, which do not work well with still-unknown threats such as zero days or APTs. It, therefore, becomes clear that there is a need for enhanced security intelligence to embrace cloud platforms.

B. Evolution of AI in Cybersecurity

AI has integrated with cybersecurity processes to the extent that threat identification and handling systems have received its influence. Supervised techniques such as machine learning are employed for other purposes, such as malware differentiation

and fraud detection, which enhance accuracy and velocity more than traditional techniques. On the other hand, unsupervised learning performs well in finding patterns that deviate from normal behaviour in the network, probably due to a new attack or an attack that is still evolving. In the same regard, there has been an improvement in threat intelligence analysis due to the application of natural language processing (NLP) to facilitate the automated extraction of useful insights from large troves of unstructured data. These conceptualisations have also shown promise in the field of proactive cybersecurity approaches.

C. Limitations of Existing AI-Based Solutions

Nonetheless, AI-based cybersecurity solutions are not without limitations. One of the important issues is increased expenses over the time needed for training and implementing complex models. Implementing such models is, to some extent, impossible in conditions of limited resource availability. Moreover, these systems remain inherently susceptible to adversarial manipulations that introduce small amendments, making AI models classify malicious activities as harmless. Another essential challenge is the interpretability of the models, often addressed as the 'black box' problem, meaning that the security analysts cannot fully trust and validate the results provided by the AI. These challenges call for additional development aimed at improving the dependence of AI solutions on knowledge and increasing their openness.

D. Research Gaps

The recent trend of developing AI methods for cloud security still has research issues requiring comprehensive and large-scale solutions. First, it lacks the fundamental conceptual structure encompassing AI as a single concept to embrace all the facets of cybersecurity, from threat assessment to vulnerability detection to response to cyber events. Furthermore, there is also a lack of attention to making models more suitable for large-scale multitenant cloud environments that require distributing resources and constructing the isolation of tenants. Another major area that has not received much attention yet understands how AI can be flexible in terms of workload demands or tenant security needs.

III. METHODOLOGY

A. Unified Framework for AI-Powered Cloud Security

The proposed unified framework places Artificial Intelligence at different levels of cloud security work processes, ensuring that work is not duplicative and can be scaled as needed. [10-15] It responds to the paramount urgency of having an integrated one covering data gathering, threat assessment, vulnerability analysis, and preventive measures.

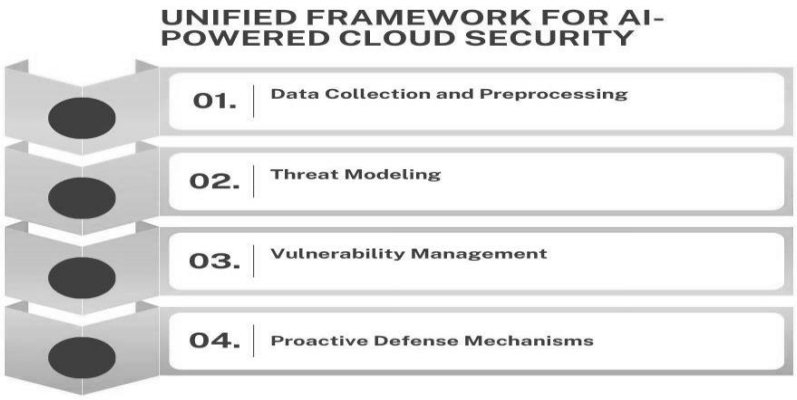

Figure 3: Unified Framework for AI-Powered Cloud Security

a) Data Collection and Preprocessing:

Information collection is the next step of the presented framework, where data is gathered from logs, net traffic, and application metrics. Ideally, this diverse database gives a holistic look at the cloud environment. Data pre-processing includes format, value scaling, and feature selection, which checks the data for punctuality and applicability. These steps enhance the performance of the subsequent AI models since much of the noise is removed and focuses on main trends.

b) Threat Modeling:

Here, threat modeling is used to identify future threats based on historical and real-time data using some of the AI methods. athematical computations analyse risks, the system's setup, and the attackers' activities to determine the areas of frustration with the architecture. Attack trees are used for this purpose and utilise the concept of graphs, which provide an easy

way to represent potential threats. This approach allows the security teams to think in the same phase as the adversaries and focus on critical aspects.

c) Vulnerability Management:

In maintaining vulnerability within the framework, automated AI tools are used to probe for exposed areas in the cloud environment. These tools first detect those misconfigurations, obsolete application versions, low-hanging fruit, etc. In We Live Secure, risks are evaluated and triaged based on the likelihood of risk exploitation, risk impact and the asset's criticality. It helps in prioritising which remediation needs to be carried out to enhance or improve to actualise the best outcome and be ready for any unfortunate mishap.

d) Proactive Defense Mechanisms:

Predictive measures work to address given situations even before they occur. The last type, unsupervised methods like clustering and anomaly detection, is applied to discover changes in organisational behaviours and new threats. The framework also includes auto-responder systems using countermeasures to isolate the impacted resources or blocklist IPs in real time. These defences help lessen the Mean Time To Detect (MTTD) and the Mean Time To Respond (MTTR) to the threats, increasing security resistance.

B. Machine Learning Models and Algorithms

Machine learning is a critically important aspect that contributes significantly to cloud security through its ability to present flexible and sophisticated solutions to identify and categorise different kinds of threats. Respective fields use different ML modelling and algorithms to make

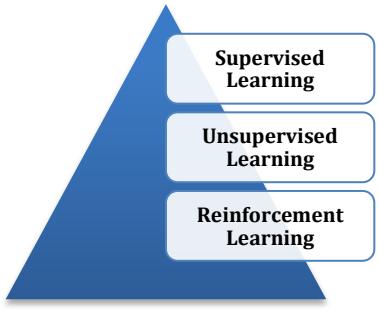

Figure 4: Machine Learning Models and Algorithms

a) Supervised Learning:

Supervised learning is especially common in classification problems, including identifying known threats like malware. Here, the model is fed on labelled data in which an input data point is mapped to the corresponding output or a predefined provided output such as malicious or benign. New data is then classified using other common algorithms such as decision trees, support vector machines, deep neural networks, etc. The benefit of the supervised learning method is the ability to correct and classify known threats because the algorithm has been trained on historical data. However, the disadvantage is the ability to deal with new unknown attack types.

b) Unsupervised Learning:

Closely related to unfamiliar or new threats, unsupervised learning can be successfully used to detect new and emerging threats based on network behaviour and system and user activity changes. Unsupervised learning is not dependent on labels, contrary to supervised learning. Contrarily, it tracks down previously untoward characteristics that produce anomalies in terms of the typical amounts of traffic, unknown system phenomena and new ways of attack. Consequently, deviation from this distribution manifests in some clusters being more compact while others are more spread out, which can easily be identified by clustering techniques, including k-means and hierarchical clustering and dimensionality reduction methods, including PCA. This makes unsupervised learning appropriate for identifying novel threats and new kinds of vulnerabilities that have not been seen before.

c) Reinforcement Learning:

Thus, reinforcement learning RL is applied to train sophisticated security policies that change with feedback in the self-check environment. This formulation is useful in an approach where an agent plays with the system, and the goal is to find the best action to improve the security status in the long run, for instance, by reducing the effects of attacks or deploying scarce

resources to counter threats. It learns by getting a reward or penalty for actions made and slowly introducing changes into decision-making. Explain how RL can be beneficial in a CLOUD COMPUTATION environment when the attacks are dynamic, and the systems' architecture also varies informally. By learning new conditions and threats, this type of learning improves security systems' effectiveness through time.

C. Tools and Technologies

As an effective solution in industry, AI cloud security depends on a set of technologies and tools that help create, evaluate and deploy ML algorithms. These tools offer the structures required to design smart systems and the infrastructures to deal with massively sized sets in cloud architecture.

a) TensorFlow and PyTorch for Developing AI Models:

TensorFlow and PyTorch are top-rated open-source tools for designing various deep learning algorithms for cloud security AI models. TensorFlow was created by Google, which is flexible and easy to scale and can be designed from basic to complex models. However, it is most effective in production settings because it can distribute models at scale easily. Pytorch, in contrast, is preferred due to its simple code and flexible computational graph and is more commonly used by researchers and developers for experimentations and future prototype model elaboration. Each framework can work with a broad array of neural networks, starting from the convolutional networks essential for image examination and continuing to the recurrent networks for sequential data analysis appropriate for cybersecurity, such as anomaly detection or malware classification.

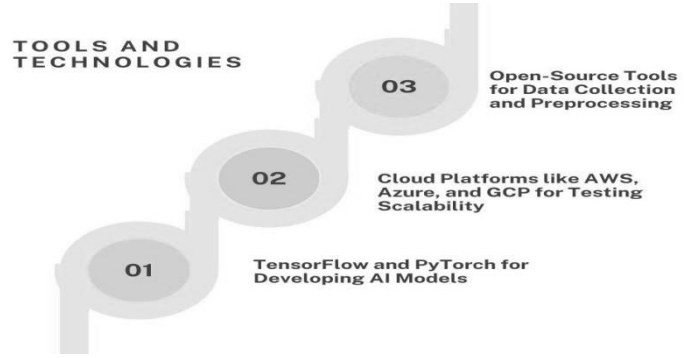

Figure 5: Tools and Technologies

b) Cloud Platforms like AWS, Azure, and GCP for Testing Scalability:

TensorFlow and PyTorch for Developing AI Models*:* TensorFlow and PyTorch are top-rated open-source tools to design various deep learning algorithms for cloud security AI models. TensorFlow was created by Google, which is flexible and easy to scale and can be designed from basic to complex models. However, it is most effective in production settings because it can distribute models at scale easily. Pytorch, in contrast, is preferred due to its simple code and flexible computational graph. Researchers and developers more commonly use it for experimentations and future prototype model elaboration. Each framework can work with a broad array of neural networks, starting from the convolutional networks essential for image examination and continuing to the recurrent networks for sequential data analysis appropriate for cybersecurity, such as anomaly detection or malware classification.

c) Open-Source Tools for Data Collection and Pre-processing:

Data acquisition tools and data pre-processing tools are often open source, two of the vital components for AI model development for cloud security. Any given system, this side of the application includes logs from servers, network devices, and applications, which are collected and aggregated in real time using Logstash, Fluentd, and Filebeat. In data cleaning or pre-processing techniques, libraries such as Pandas and NumPy in Python are used to clean and prepare data by eliminating noise, handling missing values, and extracting features. Furthermore, Apache Kafka is typically used for message brokers to handle high volumes of real-time data and Apache Spark for data computation, both ideal in large, fluctuating cloud systems. These are open source, and I can easily gather, transform, and process data vital to building AI models for cloud security.

IV. RESULTS AND DISCUSSION

A. Experimental Setup

The proposed AI-based cloud security framework was assessed in a testbed cloud environment that was set up with similar characteristics to real clouds. This configuration was intentionally designed to provide an accurate simulation of the

environment found in large-scale cloud implementations, including computing, storage, and networks. A workload model was applied to emulate the various types of operational situations that cloud environments often encounter; it imitated low-load moments, mid-load levels, and full-load conditions. This variability enabled assessing how well the factors influencing the framework adapt to different working conditions. In the security aspect of the simulation, various attacks were practised to evaluate the effectiveness of AI security defence. These scenarios included well-known threats, including conventional virus invasions and phishing scams, and unknown threats, including zero-day threats, which are security weaknesses which have not been discovered and logged. Those challenges were chosen to cover the areas of threats that cloud infrastructures can face so that the AI framework could identify known and emerging attacks. The performance of the developed framework was measured using several effectiveness parameters that are important in cloud security functions. The detection rate was evaluated to establish the AI models' ability to detect a range of malicious activities consisting of identified attacks and unidentified novel forms of attack. The FP rate was determined to establish how many harmless actions were pertaining to as risks, a key component in reducing security alerts. Last but not least, response time was carefully measured to determine how well the proposed framework can help identify and prevent particular attacks. These measurements gave a comprehensive view of the success rate of the AI-driven system developed to defend cloud systems from different types of cyber hazards.

B. Key Findings

The experimental results demonstrate the effectiveness of the AI-powered framework in various areas of cloud security.

a) Detection Accuracy:

In evaluating threat detection, the cloud security framework collaborating with AI recorded high results that showed that the models used had a 95% detection rate for known threats. This high level of accuracy is designed for familiar attack patterns, including traditional malware or signature-based threats that the system has previously encountered and entered into its database. In the case of a zero-day attack, the threat itself is new and has no signature or pattern; the AI model attained a detection rate of 87%. This is another important conclusion since it evidences the possibility of the model's spotting new and unknown threats and working without training data. This means the given system can identify other new and unnoticed risks. It was anticipated that the performance would be slightly less accurate for the zero-day threats; nonetheless, the current results are considered robust for future development, provided that more data is gathered and the model fine-tuned.

b) Vulnerability Management:

A main effectiveness was noted from the automated vulnerability scanning system uniting under the AI empowering framework in dealing with improved vulnerability. As a result, detecting and mitigating risks in cloud environments has been an intricate process that requires the utilisation of crucial manpower; this tends to be quite tiresome and may be riddled with numerous errors. On the other hand, the AI-based system we designed could routinely search through cloud resources for known vulnerabilities and could do this with a time reduction of 40% for remediation. These time-saving measures are important, particularly in open, dynamic cloud environments, where quick and timely reactions are vital to avoid risks. The further optimisation of vulnerability remediation is thus made possible by the AI system by prioritising vulnerability by risk and impact potential rather than making the process haphazard.

c) Anomaly Detection:

The AI framework incorporated an anomaly detection system that performed very well in identifying congestive Distributed Denial of Service (DDoS) attacks or those whose traffic pattern resembles normal aggregated traffic. The system placed the false positive rate below 5% to avoid wrongly throttling most of the legitimate traffic in the network. This is especially so for cloud environments because it is crucial to distinguish between permitted traffic anomalies and real attacks such as DDoS. As the system keeps false positive rates at such low levels, the alert fatigue problem is solved because the security teams spend their efforts on real threats, not on these alerts. Identifying these patterns promotes cloud systems' general security because any anomalous activity will be detected and isolated immediately.

C. Comparative Analysis

In order to evaluate distinct enhancements provided by the proposed AI-driven security framework, the outcomes were compared to mainstream cloud security solutions. At the same time, the traditional system focused more on rule-based models that include firewall and signature-based IDS; the AI-based model concentrated on smart detection and preventive defence using advanced machine learning techniques.

Table 1: Comparative Analysis

Metric	Traditional Approach	AI-Powered Approach
Detection Accuracy (%)	78	95
Remediation Time (hrs)	8	4
False Positive Rate (%)	15	5

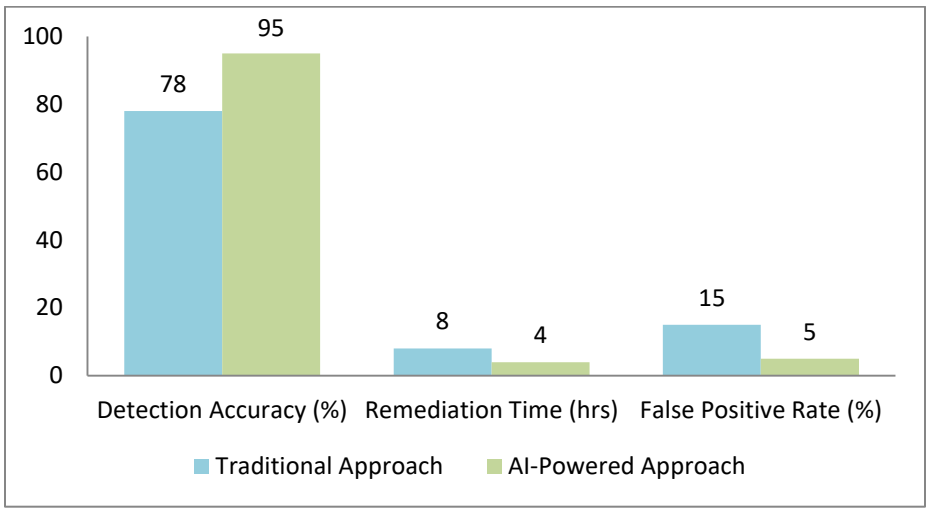

Figure 6: Graph representing Comparative Analysis

a) Detection Accuracy:

By comparing both systems, the enhanced artificial intelligence detection framework demonstrated a higher accuracy of 17% against the conventional modelling technique. In the traditional system consisting of firewalls and signature-based IDS, the detection accuracy was 78%. This implies that it failed to identify many threats, particularly those that are new or unknown to the system, such as those that do not key into any signatory data set. In contrast, the AI-powered approach established detection accuracy at 95 %, meaning machine learning models applied in the framework presented within the paper could detect a higher number of threats, including familiar and previously unknown risks, such as zero days. This significant enhancement in the detection rate proves the flexibility of AI systems to learn the new motifs of threats and provide better and more profound security in cloud networks.

b) Remediation Time:

The use of the AI-powered framework also proved that the remediation time is reduced to half: while earlier, the response usually took 8 hours, the new approach reduces it to only 4 hours. Conventional vulnerability management practices often require time-demanding manual actions, which might be inaccurate while performing in the extensive cloud environment due to human factors. On the other hand, the system developed based on AI performs vulnerability scanning and risk prioritisation through automation; this makes it easier to quickly identify critical vulnerabilities and contain them by applying remedies. This reduction in the remediation period is important in reducing the endpoint, significantly enhancing the effectiveness of cloud security response, and reducing the extent of the impact in the event of a breach.

c) False Positive Rate:

The false positive rate was also dramatically reduced by half from the conventional 15% to only 5% in the AI-incorporated system. These can be real but innocuous actions detected as a threat to the system, thus producing an alarm that may not be needed and which could interfere with the functioning of the business. The problem with using the traditional approach is that the classification between the two types of activities is not as clear, and the rate of false positives is higher due to the employment of strict rule-based systems. On the other hand, the AI system can employ machine learning algorithms to analyse default and anomalous behaviour, which reduces the number of wrong alarms. It also prevents the security operations team's overloading, making it efficient and not wasting a lot of time and resources chasing false positives.

D. Discussion on Challenges

While the results indicate substantial improvements in cloud security using AI, several challenges need to be addressed:

a) Interpretability of AI Models:

There are some well-known issues of AI models; one is the existence of the 'black box'. Although these models can attain nearly optimal performance, it is a disadvantage that a security analyst cannot always unravel why a particular action or detection was made. Such lack of transparency can compromise people's confidence in the system, especially when trapped in emergent cases that need human input.

b) Quality of Training Data:

That's why approaches based on AI models should be reviewed, as the quality of the model depends on the quality of the data on which it works. Alas, when it comes to collecting good and numerous datasets for training, the cybersecurity field has a big problem, which is much truer for case of zero-day threats or previously unforeseen attack types. Failure to obtain sufficient, and more importantly, a broad dataset would potentially hinder the model's ability to extrapolate to unseen attacks, thus affecting its performance.

c) Computational Overhead:

Security systems using AI, especially deep learning, can be computationally expensive, especially when used for real-time detection and analysis in the cloud. While cloud platforms are full of various resources that can be scaled up as needed, making the AI models computationally efficient and capable of running under limited resource conditions is a task that is still far from being solved.

V. CONCLUSION

A. Summary

Therefore, this research has identified and presented a holistic paradigm for integrating AI in cloud security to solve problems when applying conventional security mechanisms on clouds, such as accommodating dynamic workloads, identifying emerging threats, and managing vulnerabilities effectively. Machine learning for threat identification and anomaly detection has evidenced improvements in cloud security performance compared to AI-based techniques. The threat detection accuracy against known and new attacks proved high: the former was detected on average at 95%, the latter at 87%. This proves that with the help of the deployed automated vulnerability scanning system, the need for time for remediation has been cut by 40%, illustrating the efficiency of the proposed approach. In addition, it was determined that the anomaly detection system worked exceptionally well at detecting DDoS attacks with a false positive ratio of less than 5%, meaning that 'normal' traffic, not malicious, is not wrongly identified.

In conclusion, using AI in cloud security systems could greatly enhance the current detection, response, AND remediation processes. At the same time, cutting forces and overall making cloud infrastructures more robust. This approach is more beneficial and requires fewer changes as often as the clouds of the twentieth century are no longer considered safe due to varying modern threats.

B. Future Directions

Despite this work's positive findings, several significant areas deserve enhanced development to strengthen the potential of AI-empowered cloud security frameworks. First, to address the problem of opaque decision-making typical of machine learning, explainable AI (XAI) frameworks have to be employed. The use of AI in decision-making has been criticised for the lack of mechanisms that allow for tracking its decision-making process in the security field. Scientific studies directed toward constructing models that can provide readily comprehensible explanations of how they arrive at the conclusions they do would enable the security practitioners and analysts to comprehend and verify the dependability and specificity of AI-based decisions for actual application, thus there continuing to be an unending demand for advanced work in this line. Moreover, the scalability issue is still a burning one when it comes to deploying AI-based solutions in an MTaaS model wherein the resources are shared among a number of users. More such works should be directed towards improving the AI models. Hence, they operate efficiently within such systems, which pose challenges in scalability and resource availability while ensuring excellent performance and security. Some of these scalability issues may be easily solved by implementing algorithms like federated learning, which support model training on decentralised data. Lastly, scaling up the AI system with blockchain technology is worthy of future research. The decentralisation and the problems of the immutability of the blockchain can be the perfect addition to the AI models for secure data sharing and trusted decision-making. It is possible to conceptualise how these two technologies can be effectively applied together in a way that maximises the benefits that have already made blockchain appealing; for example, employing it for data verification and AI for real-time threat identification could form the basis of even more robust security architectures in the cloud.

VI. REFERENCES

[1] Walkowski, M., Oko, J., & Sujecki, S. (2021). Vulnerability management models using a common vulnerability scoring system. Applied Sciences, 11(18), 8735.

[2] Behl, A. (2011, December). Emerging security challenges in cloud computing: An insight into cloud security challenges and their mitigation. In 2011 World Congress on Information and Communication Technologies (pp. 217-222). IEEE.

[3] Stallings, W. (2015). Foundations of modern networking: SDN, NFV, QoE, IoT, and Cloud. Addison-Wesley Professional.

[4] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.

[5] Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in the cloud. Journal of network and computer applications, 36(1), 42-57.

[6] Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications surveys & tutorials, 18(2), 1153-1176.

[7] Sommer, R., & Paxson, V. (2010, May). Outside the closed world: On using machine learning for network intrusion detection. In 2010 IEEE symposium on security and privacy (pp. 305-316). IEEE.

[8] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 1-58.

[9] Li, Y., Ma, R., & Jiao, R. (2015). A hybrid malicious code detection method based on deep learning. International journal of security and its applications, 9(5), 205-216.

[10] Papernot, N., McDaniel, P., Sinha, A., & Wellman, M. (2016). Towards the science of security and privacy in machine learning. arXiv preprint arXiv:1611.03814.

[11] Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572.

[12] Ribeiro, M. T., Singh, S., & Guestrin, C. (2016, August). " Why should I trust you?" Explaining the predictions of any classifier. In Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining (pp. 1135-1144).

[13] Verma, D. C., Verma, A., & Mangla, U. (2021, December). Addressing the Limitations of AI/ML in Creating Cognitive Solutions. In 2021, IEEE third international conference on cognitive machine intelligence (CogMI) (pp. 189-196). IEEE.

[14] Bolanle, O., & Bamigboye, K. (2019). AI-Powered Cloud Security: Leveraging Advanced Threat Detection for Maximum Protection. International Journal of Trend in Scientific Research and Development, 3(2), 1407-1412.

[15] Bloch, D. A. (2023). Machine learning: Models and algorithms. Available at SSRN 4493977.

[16] García, S., Ramírez-Gallego, S., Luengo, J., Benítez, J. M., & Herrera, F. (2016). Big data preprocessing: methods and prospects. Big data analytics, 1, 1-22.

[17] Silva, V. S., Freitas, A., & Handschuh, S. (2019). On the semantic interpretability of artificial intelligence models. arXiv preprint arXiv:1907.04105.

[18] Li, X., He, K., Feng, Z., & Xu, G. (2014). Unified threat model for analysing and evaluating software threats. Security and Communication Networks, 7(10), 1454-1466.

[19] Farooqui, M. N. I., Arshad, J., & Khan, M. M. (2022). A layered approach to threat modelling for 5G-based systems. Electronics, 11(12), 1819.

[20] Chirra, D. R. (2020). AI-Based Real-Time Security Monitoring for Cloud-Native Applications in Hybrid Cloud Environments. Revista de Inteligencia Artificial en Medicina, 11(1), 382-402.