AMERICAN JOURNAL OF INNOVATION IN SCIENCE AND ENGINEERING (AJISE)

ISSN: 2158-7205 (ONLINE)

VOLUME 3 ISSUE 2 (2024)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Innovation in Science and Engineering (AJISE)

Volume 3 Issue 2, Year 2024
ISSN: 2158-7205 (Online)
DOI: https://doi.org/10.54536/ajise.v3i2.3272
https://journals.e-palli.com/home/index.php/ajise

Detecting Security System Misconfiguration Threats in Cloud Computing Environments Using AI

Hamza Mahmood Khan[1*], Syed Murtaza Haider Zaidi[2]

Article Information

Received: August 25, 2024

Accepted: September 22, 2024

Published: September 26, 2024

Keywords

Artificial Intelligence (AI), Cloud Computing, Deep Learning, HFACS Methods, Machine Learning Techniques, IRDS4C

ABSTRACT

Cloud computing solutions are being gradually adopted in organizations, and this has raised a lot of questions about the risks that come with using cloud-based services, especially misconfiguration errors in cloud-based systems. Considering these challenges, the current study aimed to assess the use of AI-based security systems to identify misconfiguration errors in cloud computing platforms. The study has focused on the perceived effectiveness of implementing AI security systems for behavioral analysis, and the implementation of traditional security systems has been assessed. The study utilized an exploratory qualitative review approach analyzing the recent studies and the recent literature available on recognized databases of interest with a particular focus on the prevalence of misconfiguration errors, its importance for early detection, and the use of AI methods. The study results showed that the most significant threat and the main reason for cloud insecurity and breaches lie in cloud misconfiguration. However, the analysis of the study also exposed that AI and machine learning techniques have a promising future and could be enacted as an accurate technique for the automation of the early misconfiguration detection model. Furthermore, the research has also pointed out that planning and deception-based approaches and human factors analysis can also be used in an attempt to strengthen cloud security against misconfiguration threats. In general, the study has postulated that the enhancement of optimum AI-based security systems is fundamental to optimizing the misconfiguration error detection systems and the security of data in cloud computing.

INTRODUCTION

The adoption of cloud service solutions has rapidly grown in the previous decade across the business fields and domains. (Buyya *et al.*, 2018). Cloud computing is a phenomenon that has changed the face of how organizations collect, store, analyze, and distribute their information and applications. Cloud computing is easily scalable, flexible, cost-efficient, and easily accessible, which makes it the most suitable for business organizations and individuals. (Zeebaree *et al.*, 2024).

The high level of growth of cloud computing can be attributed to the several advantages of adopting the technology for business needs. Hence, organizations' computing is gradually moving to the cloud, thus utilizing the cloud's capacities for the optimization of organizational processes. Research done by Markets and Markets identified the cloud computing market to be valued at $500 billion in 2024, consequently expanding at an estimated CAGR of 24%. Down to 6%, 2020 to 2024. (Markets & Markets, 2023).

Cloud misconfiguration means that proper settings have not been made while managing cloud computing resources. This may lead to data disclosure, unauthorized access, and the opening of other loopholes that hackers can exploit. (Loureiro, 2021). Errors can be implemented in the network, operating system, access control, data storage, and applications, and their impacts include unauthorized access, denial of service, violation of regulation and policy, and loss of finance. (Goel & Singhal, 2023).

The scale of cloud solutions is rising; the decentralized architecture typical of cloud services and the vast adoption of third-party cloud solutions have made hackers attracted to cloud misconfiguration (Makhdoom *et al.*, 2018). Yet, as the ongoing development of cloud computing is gradually approaching its potential, the effective setup and control of such systems are considered crucial for the present stage (Buyya *et al.*, 2018).

However, with the current increased use of cloud infrastructure, there has been an emphasis on misconfiguration errors in cloud computing environments (Bhadra & Mohammed, 2020). Misconfiguration is also observed when one is offering a cloud service where the structure is established inappropriately, making it prone to insecure threats. This is through negligence, lack of experience, and poor measures taken to protect the systems (Aurelien, 2021).

Another strategy that has emerged with equal potential for eliminating configuration errors on cloud computing systems in the past few years is artificial intelligence (AI). Security systems based on AI apply pattern matching and anomaly detection instruments to distinguish between standard and awry user interactions with the aim of threat determent. A study by Choudhary *et al.* (2023) showed that existing AI-based security systems greatly improved the effectiveness of threat identification; therefore, these are vital in cloud security (Choudhary *et al.*, 2023).

About the aforementioned parameters, the purpose of this study is to assess AI-based security solutions

[1] Westcliff University, 17877 Von Karman Ave 4th floor, Irvine, CA 92614, United States
[*] Corresponding author's e-mail: HamzaMahmoodKhan@outlook.com

to identify misconfigurations and errors relating to the use of cloud computing. Specifically, the research aims to assess the suitability of applying AI in understanding the behavior of users and traditional security solutions for cloud computing systems. This study has adopted an extensive qualitative review of the literature concerning the most recent contributions published in the last five years and retrieved from the major databases.

The importance of the proposed research is that it reveals how the use of AI security systems affects the effectiveness of threat detection and management in the cloud. Since the proposed system is AI-based, it is recommended to be implemented in a cloud computing environment to provide the highest level of data security and protection for cloud service providers, organizations, and policy-makers.

LITERATURE REVIEW

Prevalence of Misconfiguration Errors in Cloud Computing Environments

Based on previous studies, misconfiguration errors have been identified to be prevalent in cloud computing systems (Pan *et al.*, 2022; Wood & Pereira, 2010; Y. Zhang *et al.*, 2021). document by the Cloud Security Alliance reveals that misconfiguration is the leading suspected cause of cloud security breaches, making them responsible for 24% of incidents, as reflected in the cloud security breaches report. In another study by Dawood *et al.* (2023), the authors provided a quantitative estimate of cloud misconfigurations that concluded that access control errors made up nearly 70% of all the issues, and it depicts risky vulnerabilities whereby users may find themselves accessing wrong resources or information (Dawood *et al.*, 2023).

Similar research conducted by the Ponemon Institute revealed that 68% of the firms suffered a cloud-based security breach in the last year and that the vulnerability arose mostly from improper settings of the cloud solutions. (Ponemon, 2020). Also, a report by Palo Alto Networks states that the index showed that 93% of cloud storage buckets are misconfigured and publicly exposed. (Networks., 2021). Such statistics point to the catastrophe that exists in the misconfiguration issue within cloud computing and the necessity of coming up with efficient measures to solve the issue.

Early Detection of Misconfiguration Errors in Cloud Computing Environments

There are several reasons why the detection of misconfiguration errors is crucial in a cloud computing environment. First, the misconfiguration fault may cause severe effects such as the disclosure of confidential information, service disruption, or legal violation (Cornejo, 2021). For instance, identifying these risks at an early stage of the organizational activities will help the organization avoid these risks and, therefore, minimize the impact of such occurrences (Brenner *et al.*, 2023). Secondly, the cost of fixing the misconfigured errors escalates significantly with the duration of these in the system, as outlined by Westland (2002).

Likewise, in recent years, there has been an increase in the use of AI-based techniques for misconfiguration detection (Stutz *et al.*, 2024). These approaches rely more on monitoring users' behavior and then considering the probability of recognizing irregular behavior with a view to detecting threats. According to Markets and Markets research, the organizations that implement Artificial Intelligence-based security structures would be able to reduce the risk by up to 5% (Markets & , 2023).

Second, cloud structures are not only flexible but also highly dynamic, which makes it difficult to design ideal structures (Welsh & Benkhelifa, 2020). These effects should be identified at this phase if misconfiguration errors are found to avoid the continuous impact on the organization's cloud environment (Moura & Hutchison, 2020). Therefore, cost and damage due to misconfiguration errors are not compounded by each new error made, but detection is a significant challenge in cloud computing.

AI-Based Approaches for Misconfiguration Detection

Previous studies have highlighted that manual methods cannot be used to identify misconfiguration. Artificial intelligence methods are suggested. For instance, ML and deep learning models are used more often in cases where it is necessary to identify and classify misconfiguration errors in cloud environments and use them in automated decision-making processes (Ma *et al.*, 2020).

For instance, Huang *et al.* (2020) proposed a deep learning-based approach for dealing with misconfiguration errors in cloud storage services. As for the evaluation of the model, it has been indicated that for the investigated misconfiguration and permission for public access, wrong access control, or data encryption, the model reached an accuracy of more than 90 percent in most of the cases. In the same regard, Brown *et al.* (2023) presented the misconfiguration detection model that recommends an appropriate machine learning approach to execute a static and dynamic analysis automatically (Brown *et al.*, 2023). The system also proved the point that the deployed application was traceable and revealed a number of items that were scarcely configured in terms of access control, resources, and networks.

This suggests it may be feasible to extend and automate challenging misconfiguration erasures with the help of AI. Misconfiguration problems in the cloud are practical when two major approaches to artificial intelligence, namely, machine and deep learning, are applied.

Literature Gap

Despite a significant amount of effort in eradicating misconfiguration errors in the cloud computing context, some areas remain untapped and should be investigated in detail. First of all, the majority of the current studies have been conducted based on detecting misconfiguration errors in specific Cloud services or parts of them,

including Cloud storage and Cloud infrastructures. There are still no advanced systematic approaches that can be used to detect misconfigurations within an extensive spectrum of cloud computing entities and offerings (Jolkkonen, 2022).

Research Method

This study aimed to analyze the role of artificial intelligence in identifying misconfigurations of security systems in the cloud environment using a secondary exploratory review research approach. Given the nature and recent emergence of the topic, the choice of an unstructured and exploratory review type is justified, along with enhancing the review of the latest theoretical findings.

Search Strategy

This literature search for this review was carried out in several distinguished academic databases, namely, IEEE Xplore, ACM digital library, Science Direct, and Google Scholar. The search terms used were a combination of words based on the key idea of the research work, including Cloud computing, misconfiguration errors, security threats, Artificial intelligence-based detection, and Machine learning. The final selection of the articles included 41 studies covering different aspects, including challenges, integration, and opportunities associated with the employment of AI-based security systems for early detection of misconfiguration errors in cloud environments.

The search was specific to find only journal articles, conference proceedings, and industry reports published in the prior five years (2018-2023). This period is taken to avoid restriction to the latest literature as the region of cloud computing and AI-based security solutions is remodeled with technological enhancements. Therefore, the study's inclusion criteria only concerned cloud computing security on misconfiguration errors and threats studies. Additionally, the study excludes papers that describe AI-based approaches to security issues, including empirical data, case studies, or theoretical models, and are published in English only. These criteria can filter the most relevant and relevant research.

Certain papers were also excluded from the study based on criteria such as poor methodological quality, old technologies, or insufficient detail and analytical depth.

Data Analysis

All the selected studies were then critically examined and reviewed with the help of structured pattern analysis techniques. First, the purpose, methods, and findings of each study were reviewed to gain insights into its research objectives. The selected literature was systematically categorized into different themes that include- Misconfiguration Errors in Cloud Computing Environment – Overview, Prevalence of Misconfiguration Errors, Importance of Early Detection, and AI-based Misconfiguration Errors Detection Systems.

Validity of the Study

The assessment also included comparing the patterns, trends, and contradictions across selected studies and acknowledging the new approaches and the frameworks suggested for tackling the research issue.

To maintain the internal and external credibility of the review, the developed data and analysis were separately reviewed by different members of the research team. Disparities or divergence was not an issue because the participants engaged in the consensus-achieving process.

Findings

Cloud Security Challenges

Cloud computing has evolved into an essential technology by providing organizations with a means to leverage flexible and efficient computing solutions. (Battleson *et al.*, 2016). However, cloud computing architectures are complex, and so is the attack surface; these factors have created new security concerns. (Parast *et al.*, 2022).

Now, there are a plethora of security strategies that few organizations pay heed to; however, the most venerating of these security concerns about the cloud is known as cloud misconfiguration errors. (Mathews, 2017). These errors can result in critical security threats and even complicated hacking attempts by intruders. For instance, a study established that the majority, 65%, of customer cloud security breaches were due to misconfiguration, lack of proper management, and errors(Aljehani & Farooqi, 2022). Some of the biggest cloud misconfigurations that cybercriminals love to capitalize on include Weak access control, open databases, and inadequate, insecure storage buckets. (Haber *et al.*, 2022).

Another study investigated 200 cloud security incidents and discovered that the most frequent cloud configuration issues for researchers, averaging 33%, were public and cloud storage, unprotected databases, and liberal access policies. Such configurations enabled attackers to access restricted information, execute DDoS attacks, and leverage clouds' resources for performing crypto jacking. (Ismayilov, 2022).

In addition, adjustments that are frequent and conducted in the decentralized cloud setting make it nearly impossible to keep security settings uniform across multiple cloud services and geographical regions. (Uddin *et al.*, 2021) As argued by Ali *et al.* (2015), Shibli *et al.* (2014), and Loaiza Enriquez (2021), cloud misconfiguration results from problems with managing security controls, cloud structures, and the rate of change of cloud services.

To address all these issues, organizations should find it strategic to make the following changes: conduct regular security checks, have a comprehensive cloud configuration, and continuously monitor the cloud resources (Kumar & Goyal, 2019). Also, cloud providers should enhance the security to be more customer-friendly and should be able to explain to the customers how the security works in the cloud environments that the customers are subscribing to (Safonov, 2016).

Based on the trends in cloud architecture, and given that the cloud does present more attack surfaces, it is easy to see that the cloud has presented several security issues that must be addressed. It is, therefore, crucial to understand that mistakes in the configuration of the cloud are rather risky because they result in vulnerability and unique types of attacks conducted by intruders. To counter the risks outlined above, organizations should take the following measures to boost cloud security and protect their most valuable assets – data and other resources.

AI-Based Approaches for Detecting Cloud Misconfigurations

Cloud computing is a technological feature that has enhanced the storing and sharing of huge and complicated data in the last several years; nonetheless, as with every technology, it includes security concerns and challenges (Ahmadi, 2024). Among these, the misconfigurations on the cloud can be considered to be more frequent when compared to the others since they stand as a major threat to cloud security due to the openness of the systems and data (Hong *et al.*, 2019). In order to solve this problem, scientific research has been carried out to bring AI solutions into cloud environments, using machine learning and deep learning methods for the classification of threats to cloud security.

AI planning has been an area of focus in the past few years, especially in threat analysis in Cloud security. According to the present understanding, AI planning is a process of creating and selecting the right and proper plans using AI to achieve set goals (Dwivedi *et al.*, 2021). In the case of cloud protection management, the best AI planning can do is help recognize the modern improper practices and threats that are present in the cloud. For instance, the researchers have created the planning AI systems used in the evaluation of the cloud files that assist in the searching for vulnerabilities like open databases or vulnerable networks, as pointed out by Dhayanidhi (2022).

The benefits that arise from the implementation of AI planning in cloud security compared to other security systems that rely on signatures include (Sivan & Zukarnain, 2021): It is used for definite vulnerabilities or malicious intent as it does not work well when it comes to the new kinds of vulnerabilities that may occur (Li et al ., 2019). However, the A. I planning systems are not barren of the mechanism that allows them to encompass emerging threats to security, as has been said before, in consideration of the various forms of threats to security in modern society – the threshold to capture the dynamics of the threat environment. However, it can be quite useful for less specific and comparatively more detailed plans based on the state of the cloud infrastructure and possesses several open-ended risks that other tools for security cannot identify (Murturi *et al.*, 2022).

Further, regarding the benefits of utilizing AI-based solutions, it is crucial to note that the approach in question can be utilized for cloud security threats categorization and identification (Mohanty *et al.*, 2021). In traditional security, there is usually the need for people like security officers to monitor the system and look for signs of insecurity (Stutz *et al.*, 2024). However, these possibilities can be helpful in the definition and classification of such risks and threats and, therefore, contribute to faster and more effective management of security risks.

Other recent investigations have also shown how practically deployable it is to use AI for the identification of cloud misconfigurations. For example, Khalil *et al.* (2014) showed that an AI system was able to better detect cloud misconfigurations than traditional system security with 95% detection, and the traditional tools only had a 60% detection (Khalil *et al.*, 2014). Recently, in the work of Prasad *et al.*, they showed that the AI-based system can detect 80% of different threats, and traditional security tools can detect only 40%.

Hence, one can state that the use of AI techniques can be effective in identifying and classifying cloud security threats. Further, AI planning and machine learning techniques can be used to discover misconfigurations in the cloud and threats to the cloud's surroundings. However, judging by the mentioned benefits and possible drawbacks, it can be stated that the further incorporation of AI solutions to guard cloud assets is a reasonable goal for organizations that aim to enhance their cloud protection agenda.

Proposed Firewall Mechanism Using ML and DL

The proposed firewall mechanism that uses the concepts of Machine Learning (ML) and Deep Learning (DL) can be classified as one of the best solutions to enhance cybersecurity (Macas *et al.*, 2022). The proposed system combines ML with DL to give an active computable model that follows new occurrences of threats rather than the rule-based approach (Gupta *et al.*, 2019).

However, one major component of this particular generated mechanism is investigating the use of the "most frequent decision" method. This approach involves linking the ML model to a database that contains previous data so that the model learns to search for indications of certain cyber threats (Assaf & Assaad, 2023). With this approach, the system cultivates the capacity to identify the adversary's actions and also how they should be protected. Since this approach brings productivity bias towards frequently repeated decision-making patterns, the learning performance and system accuracy are enhanced, and the firewall productivity is optimized (AL Juhani, 2021; J. Zhang *et al.*, 2021).

The experiments conducted in recent studies with the UNSW-NB-15 dataset, by applying the proposed approach, successfully proved the effectiveness of the approach in case of anomaly detection (Meftah *et al.*,2019). It is a large network traffic sample that has all kinds and trends of network traffic, and this makes it a rather difficult dataset to use for benchmarking against the performance of an ADS (Vibhute *et al.*, 2024). Therefore, the performance of the proposed mechanism is quite

accurate, as seen from the outcomes of the studies above, and it is quite sensitive in distinguishing threat requests from normal ones.

However, there are certain restrictions for using this evaluation method. For example, it is possible to combine historical data, but the system does not help identify new or previously unknown types of attacks that have threatened the system for the first time (Al-Zewairi, 2021). Furthermore, the available training data may contain noise or errors, which in turn decreases the effectiveness of the system (Moualla *et al.*, 2021). In addition, the training and implementation of such a system are significantly computational in nature, which poses a concern where resources are limited in organizations (S. Wang *et al.*, 2021).

Therefore, the firewall mechanism that enhances the reinforcement of ML and DL strategies is the best approach to reinforcing the cybersecurity of automated systems. The selection of the "Most Frequent Decision" strategy complements the efficient learning rate and the system's capacity to differentiate between traditional and intrusive traffic (Marques *et al.*, 2021). Nevertheless, based on the mentioned limitations, the experiment carried out on the UNSW-NB-15 dataset confirms the high effectiveness of the method in anomaly detection (Elmrabit *et al.*, 2020). Hence, the following research gaps can be established to address the aforementioned limitations and enhance the effectiveness of this system:

Deception-Based Intrusion and Ransomware Detection

The world has become dynamic, and the use of cloud security systems has become one of the latest topics of discussion. This system is one of the advanced ways to improve the security system of cloud computing (Singh *et al.*, 2020). This strategy is known as the Intrusion and Ransomware Detection System for Cloud Computing (IRDS4C), which helps in providing the deception to find the threats (Zighan, 2024). IRDS4C is one of the well-designed models that helps in finding the difference among the different types of threats and stopping further activities, be it ransomware or intrusion. The system accepts the layers attached within the machine learning and is used in synchronizing the deep learning within the social network traffic for threat detection (El-Kosairy & Abdelbaki, 2023; X. Zhang *et al.*, 2021). This deception component is also incorporated into the system to generate fake goals to help attract the attention of attacks and learn about them (Taofeek *et al.*, 2022; Zhu *et al.*, 2021). This information is further processed and learned through the detection algorithm along with the efficiency of the system. The application of these deception-based techniques has a high potential for improving cloud security (Oluoha *et al.*, 2021). Some of the strategies that can be employed by attackers are decoy targets are created while actual targets are protected since the attackers are then busy attacking the decoys (Mohan *et al.*, 2022; Serem *et al.*, 2021). This also enables the system to gather a considerable amount of data regarding the activity pattern and approaches of the attackers that might be useful to refine the detection equations and enhance the protection measures of the cloud environment (Belal & Sundaram, 2022; Bhardwaj *et al.*, 2021).

However, this approach has some drawbacks at the same time. For example, the result of utilizing deception-based techniques significantly depends on the quality of the decoy targets as well as the number of decoy targets that exist in the system (Bojović & Lygre, 2023). If they are depicted as realistic, then perhaps they will not be attracted to such a system and, hence, be less protected. In addition, it is possible to conclude that the accuracy, which can be reached through the identified slope, as well as the efficiency of the system, may be considered as low if the training dataset includes such inaccuracies as unbalanced or different.

Hence, the actual implementation of the IRDS4C system proves the feasibility of the deception-based approaches discussed in this work in relation to cloud security and protection against cyber threats. In this process of deception, the system also gathers information about the attack, the tactics used, and strategies, hence enhancing the performance of the system (Aydeger *et al.*, 2020). Therefore, despite the weaknesses presented by the approach and the fact that advanced and enhanced deception-based schemes are used in most of the current studies, the results still seem to confirm that such types of methods can be beneficial as supplementary tools and services in the cloud security field.

Leveraging Human Factors Analysis for Cloud Misconfigurations

The Human Factors Analysis and Classification System (HFACS) has been applied in various disciplines and areas, including cloud computing, to tackle misconfiguration error risks (Ahmed *et al.*, 2024). These errors are quite challenging in cloud computing as they disable the primary protection measures that would not allow unauthorized users to access and get into the cloud system easily (Tabrizchi & Kuchaki Rafsanjani, 2020).

HFACS is a technique formally developed to classify system accidents and human errors in a complex system (Kaptan *et al.*, 2021). It is especially helpful in cloud computing since there is usually a high degree of misconfiguration because of the nature of the environment and because few people are expected to have a deep understanding of cloud computing (Nobles, 2022a). The framework is proposed to have four layers. These levels are classified as knowledge-based errors since the person lacks the relevant skills or knowledge. Secondly, there are rule-based errors that are committed when the individual fails to follow the set down rules. Also, Decision-based errors include poor decisions, which are ineffectual, and Performance-based errors, whereby the individual cannot execute the required task due to factors such as fatigue or other interferences (Nobles, 2022b).

Although cloud misconfiguration errors may seem different, they have causal pathways that can be analyzed

using HFACS and the decision-making processes at different hierarchical levels. (Kuparinen-Koho, 2020). This is in relation to the aspect of social practices, perceived self-efficacy, and attitudes toward the intended use of Cloud applications. (Wiegmann *et al.*, 2005). By doing so, the practitioners can analyze the correlation between these factors and the misconfiguration errors with an overall foundation anchored on HFACS, thus offering an avenue that covers all aspects of the human facet of cloud security.

Solving the issue of human involvement in cloud circumstances is vital since people are the cause of many misconfiguration blunders. The taxonomy of errors made available through the HFACS proves to be useful in helping analyze these errors while at the same time improving the security of cloud computing environments in the overall sense. (Belzer, 2017; Ye *et al.*, 2018). The nature of the framework allows the categorization of human errors, the tracing of potential mechanisms that lead to these mistakes, and the definition of measures that can avoid similar occurrences in the future. (Dindar *et al.*, 2020).

However, it is also necessary to note that using HFACS to address misconfiguration errors in cloud computing has certain limitations. (Nobles, 2022a). For example, in the case of an incident not previously witnessed, certain components of the framework might fail to identify them as threats. (Pandey *et al.*, 2020). Also, the system may not accomplish what it is intended to do if the training data is biased or contains errors.

In general, the wireframing of HFACS can be of great help in the formulation of a solution to the misconfiguration errors that can be encountered in the cloud computing system (Pandey *et al.*, 2020). Applying the attributes of the framework and making decisions at the different levels enables one to sever causal paths for misconfiguration errors (Nobles, 2022a). In light of this, it becomes necessary to consider human factors in cloud security since humans are central to cloud consumption; this paper has suggested the use of HFACS to this end.

DISCUSSION

The present study aimed to evaluate the effectiveness of security solutions that utilize AI in detecting configuration issues and the related misconfigurations in cloud computing environments, as well as to compare the effectiveness of applying AI in analyzing consumers' behaviors to other types of security. This current study employed the qualitative exploratory review approach to review the findings of previous literature for the purposes of the current study focusing on works done for and published in the last five years.

Moreover, it was stated that this type of threat is on the rise, especially in the cloud, and that the mentioned study looked into the potential for AI to deal with this kind of threat. It gives an understanding of the early detection of misconfiguration errors and finds thoughts that AI methods can be used to avoid additional expenses and losses caused by misconfiguration (Yungaicela-Naula *et al.*, 2024). The technique used in the identification of these technologies was searching printed scholarly databases, and only materials published within the last five years were used.

Further, it provides information on how one can employ AI security products to avoid Cloud misconfiguration threats. Aswathy & Tyagi (2022) conducted research to find different security threats that were typically related to cloud configuration issues, which have gained attention to different challenges related to data exploration and privacy violations, among others. Focusing on these study results, the repetition of the errors is because of the activities such as the security management controls and the variability of the cloud environment, which need to be treated effectively together within the different studies that were conducted at that time (Eppley, 2019).

Further, the study also focused on AI-based solutions which is another way used by the studies to explore and include the misconfiguration to resolve the challenges faced. It also focuses on discussing the various techniques that are used in ML and DL for the detection of the various types of misconfiguration errors found in cloud systems. Further, it was verified by the researchers Wu *et al.* (2020) and Abdi *et al.* (2024). These researchers worked on the detailed information that helped them to find the ways to make the security system better by using the AI-based systems that are known for their better performance as compared to traditional security tools since they have the advanced system that can detect misconfiguration more easily (Abdi *et al.*, 2024; Wu *et al.*, 2020). The study also worked on finding the advantages of the specific subfield of AI planning, focusing on the real-world use of AI-based planning within the cloud security system.

For instance, this study has revealed that AI planning systems in cloud computing form can effectively respond to dynamic threat factors, discover other threats, and formulate highly micromanipulated plans due to the conditions of cloud infrastructure – meaning that their mutual benefit over the signature-based approach has been illustrated. Automating Functionalities for Risk and Threats in security is also viewed as an advantage of AI-Asia solutions over the manual system and also supports the existence and flexibility explored by Eiras *et al.*, 2024). Lastly, this study has investigated the comparison between the proposed firewall mechanism and the two different structures in recent studies that employed both machine learning and deep learning for enhanced cloud security. The aforementioned concept of the 'most frequent decision' appears to be very useful in increasing learning performance and making the system more reliable to eliminate unwanted or perhaps potential malicious traffic. However, there are some weaknesses, such as the direction of possible biased or erroneous training data and high computational expense, where this study comes up with an effective approach from the results established using the UNSW-NB-15 dataset.

Moreover, the study further strengthens the idea of

AI-based security solutions in the context of cloud computing by highlighting deception-based intrusion and ransomware detection frameworks, namely IRDS4C. They involve the deployment of tricks to lure and monitor attackers, the layered format, and the utilization of machine learning and deep learning, which also establishes these advanced security systems as intelligent and versatile. (Okafor *et al.*).

In summary, the research offered a broad understanding of cloud misconfiguration risks and the efficiency of AI security measures. It guides how to apply an Artificial Intelligence approach to the security of cloud computing systems and data. Through the analysis of current scientific literature and continuous critical evaluation of approaches, the article reveals the strengths of AI-based solutions, which provide the ability to learn from threats, identify weaknesses, and advance threat recognition and mitigation. In general, this study could serve as the basis for further research and development of this type of cloud computing security technology.

CONCLUSION

The present study has established that cloud misconfiguration is a common and sensitive concern, with research suggesting that it is responsible for 70% of cloud security vulnerabilities. Such misconfigurations must be detected as early as possible to avoid the possible repercussions and expenses that come with it. Applications such as machine learning and deep learning in the AI approach have emerged as a better way of auto-detecting and categorizing cloud misconfiguration threats from other security threats more accurately than traditional approaches. Also, there are new methods of intrusion detection based on the deception of attackers, and the analysis of human factors complements existing methods to improve the security of cloud services. The study has limitations, including its reliance on qualitative literature review methods, which may introduce bias and limit the generalizability of findings. Additionally, the focus on specific cloud services may overlook broader misconfiguration issues across diverse cloud environments. Future research should explore systematic approaches for detecting misconfigurations across various cloud platforms and integrate empirical data to validate AI-based detection methods. In sum, the research emphasizes AI's potential as a critical factor that can help solve the problem of cloud misconfiguration.

REFERENCES

Abdi, A. H., Audah, L., Saleh, A., Alhartomi, M. A., Rasheed, H., Ahmed, S., & Tahir, A. (2024). Security Control and Data Planes of SDN: A Comprehensive Review of Traditional, AI and MTD Approaches to Security Solutions. *IEEE Access*.

Abouelyazid, M., & Xiang, C. (2019). Architectures for AI Integration in Next-Generation Cloud Infrastructure, Development, Security, and Management. *International Journal of Information and Cybersecurity, 3*(1), 1-19.

Ahmadi, S. (2024). Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. Ahmadi, S.(2024) Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *Journal of Information Security, 15,* 148-167.

Ahmed, M., Kambam, H. R., Liu, Y., Jaidka, S., & Petrova, K. (2024). Impact and Significance of Human Factors in Digital Information Security. *International Journal of Information Science and Technology, 7*(2), 1-17.

Al-Zewairi, M. A. S. (2021). A novel multilayer IDS architecture for learning undefined attacks. *Princess Sumaya University for Technology*.

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information sciences, 305,* 357-383.

Aljehani, S., & Farooqi, N. S. (2022). A Systematic Literature Review on Security Challenges In A Hybrid Cloud Database. *International Journal of Engineering & Technology*.

Aljuhani, A. (2021). Machine learning approaches for combating distributed denial of service attacks in modern networking environments. *IEEE Access, 9,* 42236-42264.

Alliance., C. S. (2019). *Cloud Security Report.* https://cloudsecurityalliance.org/artifacts/cloud-security-report-2019/

Assaf, G., & Assaad, R. H. (2023). Key decision-making factors influencing bundling strategies: Analysis of bundled infrastructure projects. *Journal of Infrastructure Systems, 29*(2), 04023006.

Aswathy, S., & Tyagi, A. K. (2022). Privacy Breaches through Cyber Vulnerabilities: Critical Issues, Open Challenges, and Possible Countermeasures for the Future. In *Security and Privacy-Preserving Techniques in Wireless Robotics* (pp. 163-210). CRC Press.

Aurelien, J. (2021). Exploring effective defensive cybersecurity strategies for small businesses. *Colorado Technical University*.

Aydeger, A., Saputro, N., & Akkaya, K. (2020). Cloud-based deception against network reconnaissance attacks using SDN and NFV. In *2020 IEEE 45th Conference on Local Computer Networks* (LCN).

Battleson, D. A., West, B. C., Kim, J., Ramesh, B., & Robinson, P. S. (2016). Achieving dynamic capabilities with cloud computing: An empirical investigation. *European Journal of Information Systems, 25*(3), 209-230.

Belal, M. M., & Sundaram, D. M. (2022). A comprehensive review on intelligent security defenses in the cloud: Taxonomy, security issues, ML/DL techniques, challenges, and future trends. *Journal of King Saud University-Computer and Information Sciences, 34*(10), 9102-9131.

Belzer, J. A. (2017). Unmanned aircraft systems in the national airspace system: Establishing equivalency in safety and training through a fault tree analysis

approach. *Ohio University.*

Bhadra, S., & Mohammed, S. (2020). Cloud computing threats and risks: Uncertainty and uncontrollability in the risk society. *Electronics Journal, 7*(2), 1047-1071.

Bhardwaj, A., Mangat, V., Vig, R., Halder, S., & Conti, M. (2021). Distributed denial of service attacks in the cloud: State-of-the-art of scientific and commercial solutions. *Computer Science Review, 39,* 100332.

Bojović, D., & Lygre, J. T. (2023). To deceive or not deceive: Unveiling the adoption determinants of defensive cyber deception in Norwegian organizations. *University of Agder.*

Bramer, W. M., De Jonge, G. B., Rethlefsen, M. L., Mast, F., & Kleijnen, J. (2018). A systematic approach to searching: an efficient and complete method to develop literature searches. *Journal of the Medical Library Association: JMLA, 106*(4), 531.

Brenner, B., Hollerer, S., Bhosale, P., Sauter, T., Kastner, W., Fabini, J., & Zseby, T. (2023). Better safe than sorry: Risk Management based on a safety-augmented Network Intrusion Detection System. *IEEE Open Journal of the Industrial Electronics Society.*

Brown, A., Gupta, M., & Abdelsalam, M. (2023). Automated machine learning for deep learning based malware detection. *arXiv.* https://doi.org/10.48550/arXiv.2303.01679

Buyya, R., Srirama, S. N., Casale, G., Calheiros, R., Simmhan, Y., Varghese, B., Gelenbe, E., Javadi, B., Vaquero, L. M., & Netto, M. A. (2018). A manifesto for future generation cloud computing: Research directions for the next decade. *ACM computing surveys (CSUR), 51*(5), 1-38.

Choudhary, C., Vyas, N., & Kumar Lilhore, U. (2023). Cloud Security: Challenges and Strategies for Ensuring Data Protection. In *2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS),* 669-673.

Cornejo, G. A. (2021). Human errors in data breaches: An exploratory configurational analysis. *Nova Southeastern University.*

Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M., & Rehman, S. U. (2023). Cyberattacks and security of cloud computing: a complete guideline. *Symmetry, 15*(11), 1981.

Dhayanidhi, G. (2022). Research on IoT threats & implementation of AI/ML to address emerging cybersecurity issues in IoT with cloud computing. *IEEE Access.*

Dindar, S., Kaewunruen, S., & An, M. (2020). Bayesian network-based human error reliability assessment of derailments. *Reliability Engineering & System Safety, 197,* 106825.

Dunn, C., Moustafa, N., & Turnbull, B. (2020). Robustness evaluations of sustainable machine learning models against data poisoning attacks in the Internet of things. *Sustainability, 12*(16), 6434.

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., & Eirug, A. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice, and policy. *International Journal of Information Management, 57,* 101994.

Eiras, F., Petrov, A., Vidgen, B., Schroeder, C., Pizzati, F., Elkins, K., Mukhopadhyay, S., Bibi, A., Purewal, A., & Botos, C. (2024). *Risks and Opportunities of Open-Source Generative AI.* arXiv preprint arXiv:2405.08597.

El-Kosairy, A., & Abdelbaki, N. (2023). Deception as a service: intrusion and ransomware detection system for cloud computing (IRDS4C). *Advances in Computational Intelligence, 3*(3), 9.

Elmrabit, N., Zhou, F., Li, F., & Zhou, H. (2020). Evaluation of machine learning algorithms for anomaly detection. In *Proceedings of the 2020 International Conference on Cyber Security and Protection of Digital Services* (Cyber Security).

Eppley, E. (2019). *Critical success factors for digital forensic investigations in cloud computing: An exploratory multiple-case study* [Doctoral dissertation, Capella University].

Goel, P. K., & Singhal, A. (2023). Security issues and threats in cloud computing: Problems and solutions. In *Proceedings of the 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE)* (pp. 1019-1023).

Gupta, A., Anpalagan, A., Carvalho, G. H., Khwaja, A. S., Guan, L., & Woungang, I. (2019). RETRACTED: Prevailing and emerging cyber threats and security practices in IoT-enabled smart grids: A survey. *Elsevier.*

Haber, M. J., Chappell, B., & Hills, C. (2022). Attack vectors. In *Cloud attack vectors: Building effective cyber-defense strategies to protect cloud resources* (pp. 117-219). Springer.

Hong, J. B., Nhlabatsi, A., Kim, D. S., Hussein, A., Fetais, N., & Khan, K. M. (2019). Systematic identification of threats in the cloud: A survey. *Computer Networks, 150,* 46-69.

Ismayilov, E. A. (2022). Cloud security: A review of current issues and proposed solutions. *Azerbaijan Journal of High Performance Computing.*

Jolkkonen, T. (2022). *Cloud Asset Identification Strategy.*

Kaptan, M., Sarıalïoğlu, S., Uğurlu, Ö., & Wang, J. (2021). The evolution of the HFACS method used in the analysis of marine accidents: A review. *International Journal of Industrial Ergonomics, 86,* 103225.

Khalil, I., Khreishah, A., & Azeem, M. (2014). *Cloud Computing Security: A Survey. Computers, 3,* 1-35. https://doi.org/10.3390/computers3010001

Kumar, R., & Goyal, R. (2019). Assurance of data security and privacy in the cloud: A three-dimensional perspective. *Software Quality Professional, 21*(2), 7-26.

Kuparinen-Koho, T. (2020). *Risks in the user interaction of alarm functionality in situation awareness systems.*

Li, W., Tug, S., Meng, W., & Wang, Y. (2019). Designing collaborative blockchain signature-based intrusion detection in IoT environments. *Future Generation Computer Systems, 96,* 481-489.

Loaiza Enriquez, R. (2021). *Cloud Security Posture Management/CSPM) in Azure.*

Loureiro, S. (2021). Security misconfigurations and how to prevent them. *Network Security, 2021*(5), 13-16.

Ma, X., Zhou, A., Zhang, S., & Wang, S. (2020, 6-9 July 2020). *Cooperative Service Caching and Workload Scheduling in Mobile Edge Computing*. IEEE INFOCOM 2020 - IEEE Conference on Computer Communications,

Macas, M., Wu, C., & Fuertes, W. (2022). A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. *Computer Networks, 212,* 109032.

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2018). Anatomy of threats to the Internet of Things. *IEEE communications surveys & tutorials, 21*(2), 1636-1675.

MarketsandMarkets. (2023). *Cloud computing market size, share, growth drivers, opportunities & statistics*. https://www.marketsandmarkets.com/Market-Reports/cloud-computing-market-234.html

Marques, C., Malta, S., & Magalhães, J. (2021). DNS firewall based on machine learning. *Future Internet, 13*(12), 309.

Mathews, R. (2017). Interrogating "privacy" in a world brimming with high political entanglements, surveillance, interdependence & interconnections. In *Vol. 7* (pp. 265-324). Springer.

Meftah, S., Rachidi, T., & Assem, N. (2019). Network-based intrusion detection using the UNSW-NB15 dataset. *International Journal of Computing and Digital Systems, 8*(5), 478-487.

Mohan, P. V., Dixit, S., Gyaneshwar, A., Chadha, U., Srinivasan, K., & Seo, J. T. (2022). Leveraging computational intelligence techniques for defensive deception: a review, recent advances, open problems, and future directions. *Sensors, 22*(6), 2194.

Mohanty, S. N., Potluri, S., Prakash, V. B., Srinath, B., & Manjunath, B. (2021). Cloud security concepts, threats, and solutions: Artificial intelligence based Approach. *Cloud Security: Techniques and Applications, 1,* 1.

Moualla, S., Khorzom, K., & Jafar, A. (2021). Improving the Performance of Machine Learning-Based Network Intrusion Detection Systems on the UNSW-NB15 Dataset. *Computational Intelligence and Neuroscience, 2021*(1), 5557577.

Moura, J., & Hutchison, D. (2020). Fog computing systems: State-of-the-art research issues and future trends, with a focus on resilience. *Journal of Network and Computer Applications, 169,* 102784.

Murturi, I., Egyed, A., & Dustdar, S. (2022). Utilizing AI Planning on the Edge. *IEEE Internet Computing, 26*(2), 28-35. https://doi.org/10.1109/MIC.2021.3073434

Networks., P. A. (2021). *Cloud Threat Report*. https://www.paloaltonetworks.com/resources/research/cloud-threat-report

Nobles, C. (2022a). Investigating cloud computing misconfiguration errors using the human factors analysis and classification system. *Scientific Bulletin, 27*(1), 59-66.

Nobles, C. (2022b). Investigating Cloud Computing Misconfiguration Errors using the Human Factors Analysis and Classification System. *Scientific Bulletin, 27,* 59 - 66.

Okafor, W., Okafor, K. C., Edeagu, S., Chijindu, V., & Iloanusi, O. N. Efficient Container Time Synchronization Data Center Network for Smart Grid Cyber-Physical Architecture. O. and Chijindu, Vincent. C. and Iloanusi, Ogechukwu N., Efficient Container Time Synchronization Data Center Network for Smart Grid Cyber-Physical Architecture.

Oluoha, O. U., Yange, T. S., Okereke, G. E., & Bakpo, F. S. (2021). Cutting Edge Trends in Deception Based Intrusion Detection Systems—A Survey. *Journal of Information Security, 12*(4), 250-269.

Pan, H., Li, Z., Zhang, P., Cui, P., Salamatian, K., & Xie, G. (2022). Misconfiguration-Free Compositional SDN for Cloud Networks. *IEEE Transactions on Dependable and Secure Computing.*

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing, 13*(1), 103-128.

Parast, F. K., Sindhav, C., Nikam, S., Yekta, H. I., Kent, K. B., & Hakak, S. (2022). Cloud computing security: A survey of service-based models. *Computers & Security, 114,* 102580.

Ponemon, L. (2020). *Cost of a Data Breach Report 2019*. IBM Security.

Prasad, N., Lopes, J., Shah, U., Narukulla, N., & Swamy, H. (2022). Security Challenges and Solutions in Cloud-Based Artificial Intelligence and Machine Learning Systems. *International Journal on Recent and Innovation Trends in Computing and Communication, 10,* 286-292.

Safonov, V. O. (2016). *Trustworthy cloud computing*. John Wiley & Sons.

Serem, E. K., Mugo, D. M., & Too, B. K. (2021). Deceptive decoys: Combining believable user and network activities and deceptive network setup in enhancing effectiveness. *Technology (IJEET), 12*(6), 281-292.

Shibli, M. A., Masood, R., Habiba, U., Kanwal, A., Ghazi, Y., & Mumtaz, R. (2014). Access control as a service in the cloud: challenges, impact, and strategies. *Continued Rise of the Cloud: Advances and Trends in Cloud Computing,* 55-99.

Singh, P., Kaur, A., Aujla, G. S., Batth, R. S., & Kanhere, S. (2020). Daas: Dew computing is a service for intelligent intrusion detection in edge-of-things ecosystems. *IEEE Internet of Things Journal, 8*(16), 12569-12577.

Sivan, R., & Zukarnain, Z. A. (2021). Security and privacy in a cloud-based e-health system. *Symmetry, 13*(5), 742.

Stutz, D., de Assis, J. T., Laghari, A. A., Khan, A. A., Andreopoulos, N., Terziev, A., Deshpande, A., Kulkarni, D., & Grata, E. G. (2024). Enhancing security in cloud computing using artificial intelligence (AI). In *Applying artificial intelligence in cybersecurity*

analytics and cyber threat detection (pp. 179-220). Springer.

Symon, G., Cassell, C., & Johnson, P. (2018). Evaluative practices in qualitative management research: A critical review. *International Journal of Management Reviews, 20*(1), 134-154.

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing, 76*(12), 9493-9532.

Taofeek, O. T., Alawida, M., Alabdulatif, A., Omolara, A. E., & Abiodun, O. I. (2022). A cognitive deception model for generating fake documents to curb data exfiltration in networks during cyber-attacks. *IEEE Access, 10,* 41457-41476.

Uddin, M., Khalique, A., Jumani, A. K., Ullah, S. S., & Hussain, S. (2021). Next-generation blockchain-enabled virtualized cloud security solutions: review and open challenges. *Electronics, 10*(20), 2493.

Vibhute, A. D., Khan, M., Patil, C. H., Gaikwad, S. V., Mane, A. V., & Patel, K. K. (2024). Network anomaly detection and performance evaluation of Convolutional Neural Networks on UNSW-NB15 dataset. *Procedia Computer Science, 235,* 2227-2236.

Wang, L., Han, M., Li, X., Zhang, N., & Cheng, H. (2021). Review of classification methods on unbalanced data sets. *IEEE Access, 9,* 64606-64628.

Wang, S., Zhu, F., Yao, Y., Tang, W., Xiao, Y., & Xiong, S. (2021). A computing resources prediction approach based on ensemble learning for complex system simulation in the cloud environment. *Simulation Modelling Practice and Theory, 107,* 102202.

Welsh, T., & Benkhelifa, E. (2020). On resilience in cloud computing: A survey of techniques across the cloud domain. *ACM computing surveys (CSUR), 53*(3), 1-36.

Westland, J. (2002). The cost of errors in software development: evidence from industry. *Journal of Systems and Software, 62,* 1-9. https://doi.org/10.1016/S0164-1212(01)00130-3

Wiegmann, D., Faaborg, T., Boquet, A., Detwiler, C., Holcomb, K., & Shappell, S. (2005). Human error and general aviation accidents: A comprehensive, fine-grained analysis using HFACS.

Wood, K., & Pereira, E. (2010). An investigation into cloud configuration and security. 2010 International Conference for Internet Technology and Secured Transactions.

Wu, H., Han, H., Wang, X., & Sun, S. (2020). Research on artificial intelligence enhancing internet of things security: A survey. *IEEE Access, 8,* 153826-153848.

Ye, G., Tan, Q., Gong, X., Xiang, Q., Wang, Y., & Liu, Q. (2018). Improved HFACS on human factors of construction accidents: a China perspective. *Advances in Civil Engineering, 2018*(1), 4398345.

Yungaicela-Naula, N. M., Sharma, V., & Scott-Hayward, S. (2024). Misconfiguration in O-RAN: Analysis of the impact of AI/ML. *Computer Networks,* 110455.

Zeebaree, I., Abdulrahman, L. M., Abdulkareem, N. M., & Salim, B. W. (2024). The Distributed Machine Learning in Cloud Computing and Web Technology: A Review of Scalability and Efficiency. *Journal of Information Technology and Informatics, 3*(1).

Zhang, J., Pan, L., Han, Q.-L., Chen, C., Wen, S., & Xiang, Y. (2021). Deep learning based attack detection for cyber-physical system cybersecurity: A survey. *IEEE/CAA Journal of Automatica Sinica, 9*(3), 377-391.

Zhang, X., Wang, J., & Zhu, S. (2021). Dual generative adversarial networks based on unknown encryption ransomware attack detection. *IEEE Access, 10,* 900-913.

Zhang, Y., He, H., Legunsen, O., Li, S., Dong, W., & Xu, T. (2021). An evolutionary study of configuration design and implementation in cloud systems. In *2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE).*

Zhu, M., Anwar, A. H., Wan, Z., Cho, J.-H., Kamhoua, C., & Singh, M. P. (2021). Game-theoretic and machine learning-based approaches for defensive deception: A survey. *arXiv preprint arXiv:2101.10121.* https://arxiv.org/abs/2101.10121

Zighan, S. (2024). Navigating the cyber landscape: A framework for transitioning from business continuity to digital resilience. In *2024 2nd International Conference on Cyber Resilience (ICCR)* (pp. TBD). IEEE.