International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

Threat Detection and Incident Response in the Cloud

Venkata Soma

New York Mets

Abstract: ***In the emerging landscape of cyber-attacks, the incorporation of threat detection and incident response becomes paramount within the cloud environment. This research focuses on the exploration of multifaceted aspects of threat detection and incident responses within the cloud environment, especially focusing on the sports industry. This analyses the present strategies and addresses the potential gaps and provides innovative solutions for the enhancement of the cloud security settings. Despite the significant scalability and flexibility and flexibility offered through cloud computing, various unique security challenges arise in these areas. This study emphasises the integration of threat detection and incident response processes for the improvement of risk mitigation techniques and real-time monitoring. Future work in this area will be focused on the integration of cloud-native and empirical validation for the improvement of cloud environments.***

Keywords: Cloud Security, Incident Response, Threat Detection, Cybersecurity, Cloud Computing Strategies, Cloud Environments, Security Posture

1. Introduction

The requirement for vigorous threat detection and incident response becomes essential for organisations, particularly within the sports industry because the IT infrastructure expands rigorously. Despite offering streamlined flexibility and scalability, cloud environments pose unique security challenges [1].

a) Project Specification

This research tries to explore multifaceted aspects of the threat detection process along with the response to various incidents within the cloud environment. This study focuses on the analysis of existing measures of threat detection and the identification of potential gaps to propose innovative solutions for the enhancement of the security position.

b) Aims and Objectives

Aim

This research aims to analyse the threat detection process and incident responses for the enhancement of security within cloud environments.

Objectives

- To identify the potential threats within the existing cloud security
- To assess the current threat detection and incident response strategies within the cloud settings
- To provide recommendations for the organisations for the improvement of cloud security postures

c) Research Questions

- What are the current strategies for threat detection and incident response within cloud environments?
- What is the impact of the proposed strategies on the overall security of the cloud environment?
- What are the main challenges and limitations related to these strategies?

d) Research Rationale

The increasing adoption of cloud computing changes the way how organisations operate and offers unparalleled levels of flexibility, cost-effectiveness and scalability. The threat detection process reveals the potential security risks by including activities which indicate the devices, networks and software are compromised [2]. On the other hand, incident response includes the steps for the security team and the automated tools that are used for mitigating cyber threat issues. The dynamic nature of the cloud environments highlights the rethinking of threat detection and response accordingly. Through the enhancement of the understanding of cloud-specific understandings and threats, this research paper contributes to the development of a more flexible cloud infrastructure.

2. Literature Review

a) Research background

In the present state of cloud computing, it is necessary to provide flexible and scalable resources which support a broader range of business applications. Despite that, this transformation delivers new security challenges, especially in threat detection and automated incident response within the sports industry. The traditional security measures are not adequate within the cloud environment in which the allocation of resources and the decentralised nature of the cloud infrastructure are not streamlined properly [3]. The rationale of this research lies within the requirement of the efficiency and adaptive threat detection process along with the *response to various incidents within the cloud environment.*

b) Critical assessment

Though the cloud environment delivers significant flexibility along with scalability, some significant challenges hinder its effectiveness. This issue includes the complications within the data security across various locations, conventional response to the emerging threats and the management of access control. The threat detection and incident response processes include the detection of potential threats,

investigation of uncertainties, elimination of root causes and incorporation of actionable measures for eliminating potential risks [4].

c) Linking with aim

This research seeks to evaluate and develop innovative strategies for detection of threats and incident responses within the cloud environment. Cloud security threat detection includes the identification and response to emerging cyber threats within the cloud environments through leveraging cloud-native techniques and instruments. The main goal is to deliver organisations with practical, scalable and streamlined solutions for the improvement of their capability to detect threats and provide responses within the real-time phenomenon.

d) Encapsulation of applications

The applications of this research are rooted in the wider area which assists in the improvement of threat detection and incident response mechanisms which can be applied across various industries which rely on cloud-based services, especially the sports industry. Through the enhancement of security within the cloud environments, this research contributes significantly to the protection of sensitive and informative data [5]. In addition to this, the proposed solutions can be integrated with the existing security operation centres and the cloud management platforms. This further provides organisations with incident response tools which are both effective and easy to incorporate.

e) Theoretical framework

The theoretical framework of this study encompasses various theories such as incident response lifecycle, principles of cloud security architecture and machine learning for cybersecurity. The cloud security architecture framework delivers a foundation for understanding the unique challenges of securing cloud environments [6]. On the contrary, the incident response lifecycle of the organisational process reacts to IT threats such as cyberattacks, server downtime and security breaches. The security of the network is the fundamental base for cloud security measures. This includes the implementation of the cloud-based barriers and security groups for controlling the inbound and outbound traffic [7].

f) Literature gap

Despite of vast varied enriched literature on cloud security, there are significant gaps in the areas of threat detection along with incident response. The existing studies focus on either incident response or detection of potential threats without including the integration of these functions within the cloud-specific contexts. In addition to this, there exists a lack of research on the application of machine learning in real-time threat management in cloud settings.

3. Methodology

a) Research Philosophy

The incorporation of the interpretivism research philosophy within this research assists in the analysis of data related to human activities in response to cyber threats. This research allows the researchers to understand the thoughts and feelings of the individual about the detection of emerging threats and incident responses. This philosophy assists in the exploration of human behaviour in response to cyber threats and recognising the actionable techniques for the detection of threats and responding to the various events within the cloud environment.

b) Research Approach

This paper employed a deductive research approach which assists in the exploration of the potential cyber threats and provides a response to multiple incidents by incorporating various theories. The utilisation of the deductive research approach assists the researchers in generalising their ideas and then testing these through the incorporation of specific observations.

c) Research design

In this study, the qualitative research design is incorporated for the specification of qualitative insights about threat detection techniques and incident response within the cloud-based areas. This research design analyses the scenario-based methodology which underlines the different threats and incident responses for providing fruitful answers to the research questions.

d) Data collection method

The peer review data collection method is used in this research for discussing the information about emerging threats and incident response tools collected from different literature, journals and articles. The peer-review process assists in ensuring that the used articles and journals deliver accurate, accountable and actionable contributions to treatment detection within the cloud environment. It also contributes to the prevention of personal biases from affecting the outcomes of various threat detection techniques and incident response within cloud-based services.

e) Ethical consideration

In the cybersecurity and cloud environments, ethical consideration includes the assurance of privacy, transparency, accountability and fairness for handling the data, implementing these security measures and responding to threats. It ensures the implementation of the vigorous security measures and response to the threats as well.

4. Results

a) Critical analysis

This research provides actionable insights into threat detection and incident response within cloud environments, nevertheless, there exist significant gaps. Many studies focus on specific cloud service providers which restrict the transferability of the findings across different cloud platforms. In addition to this, the reliance on artificial intelligence and machine learning disregarded the issues in the implementation of the technologies to scale. The intricate interplay between the security measures provided by cloud providers and internal security controls provided by organisations expands the way for further assessment [8].

b) Findings and discussion

Theme 1: Potential threats within the existing cloud security

Cloud security bases hold significant issues that hinder the effectiveness of cloud services across multiple cloud channels. One of the major issues in cloud security is the

misconfiguration which leads to a significant amount of data breaches [9]. Within the sports industry, the inadequacy in security posture management, reliance on cloud service providers and limited visibility offers significant issues that pose significant challenges. The ease of the usage of the cloud in combination with the complication of multi-cloud environments makes the security cloud environment more challenging. The CSPs offer well-documented APIs for providing ease of customer use, despite these benefits, they pose a risk to property security [10]. Cybercriminals can be able to exploit similar documentation for the identification of potential vulnerabilities and access to sensitive data.

Theme 2: Current threat detection and incident response strategies within the cloud settings

Threat detection and response is essential through incorporating the collaborative process which supports the security of the cloud environments. The threat detection process focuses on the collation of data for the identification of emerging threats and the incident responses leverage the data for the execution of the remedial actions [11]. The primary benefit of this collaborative approach is the continuous monitoring of the growing threats. The threat detection operates as per a pattern which assists in ensuring that the cloud environment is monitored constantly and capable of addressing the risks according to its emergence. The coordinated response is another benefit which helps to gain threat detection abilities directly from the responsive strategy [12]. It further enables timely and precise actions for the mitigation of identified risk factors. The ongoing attention plays a crucial role in the maintenance of strong security postures within the ever-evolving area of cyber threats. The integration of the threat detection process and incident response leads to a significant improvement in the security positioning within the cloud environments.

Theme 3: Impact of the proposed strategies on the overall security of the cloud environment

Successful implementation of security measures within the cloud settings is necessary for enhancing the credibility of the threat detection processes and incident response. It includes the development of technologies for the monitoring, encryption and management of potential vulnerabilities. The implementation of the overall processes secures the cloud environments against emerging cyber-attacks and weaknesses. The cloud security strategies assist in the documentation of cloud computing, exploration of the various cloud services and showcase the cloud security frameworks [13]. Cloud computing strategies deliver computing strategies over the internet. Various cloud service models such as the "*Infrastructure as a Service*" (IaaS), "*Software as a Service*" (SaaS) and "*Platform as a Service*" (PaaS) assist in this regard. The IaaS delivers visualised computing resources, and the PaaS offers different hardware and software instruments for application development. The SaaS provides software applications over the Internet [14].

c) Evaluation

The research on threat detection and incident response within the cloud environments is essential for the increase in the adoption of cloud technologies within the evolving cybersecurity landscape. This study highlights the unique challenges within the cloud environments that include the complications within the multi-cloud architectures. In this area, the significance of artificial intelligence, machine learning, and automation holds an important exertion for the enhancement of threat detection abilities [15]. The increasing pace of evaluation of cloud technologies means that the research become antiquated which underlines the essentiality of repetitive approaches.

5. Conclusion

In conclusion, threat detection and incident response within the cloud environments are essential for protecting the organisational data and the maintenance of operational clarity. The dynamic nature of the cloud combined with the evolving threat detection environment. This necessitates advanced detection and response techniques. This research made a significant aspect in the understanding and identification of these challenges which assist in bridging the gap in this area. This ensures comprehensive security within the cloud environments that require continuous adoption, integration of the automated instruments and connectivity between the cloud service providers.

6. Research Recommendation

It is recommended that the research shroud emphasis on the development of the standardised framework for threat detection and incident response. The emphasis must be focused on the construction of practical and streamlined solutions which have been incorporated the artificial intelligence and machine learning. This will further boost the accuracy of threat detection processes while eliminating security issues. In addition to this, further work must traverse the integration of the cloud-native security mechanisms with third-party solutions for providing a holistic security position. The interconnectivity between the cloud service providers and the sports industry is essential for the validation and refinement of the framework within real-life phenomena.

7. Future Work

Future work in this area must focus on the empirical studies which assist in the validation and testing the threat detection and incident response strategies within various cloud environments. Further research should identify the efficacy of AI-driven threat intelligence sharing across the cloud ecosystems. It enables vigorous defence mechanisms and the development of more streamlined tools for real-time monitoring. The incorporation of the automated incident response fosters the culture of tailoring the specific requirements of the cloud process. In addition to this, future efforts must identify the legal and regulatory issues within the incident responses within the international cloud deployments. IT assist in ensuring regulatory compliance and data integrity while maintaining vigorous security.

References

[1] A. Alshammari, S. Alhaidari, A. Alharbi, and M. Zohdy, "Security threats and challenges in cloud computing," in *Proc. 2017 IEEE 4th Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)*, 2017, pp. 46-51.

Available: https://ieeexplore.ieee.org/abstract/document/7987175/

[2] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Netw.*, vol. 169, p. 107094, 2020. Available: https://www.sciencedirect.com/science/article/pii/S1389128619311235.

[3] P. Raj and A. Raman, "Multi-cloud management: Technologies, tools, and techniques," in *Software-Defined Cloud Centers: Operational and Management Technologies and Tools*, P. Raj and A. Raman, Eds. Cham: Springer, 2018, pp. 219-240. Available: https://link.springer.com/chapter/10.1007/978-3-319-78637-7_10.

[4] W. Bautista, *Practical cyber intelligence: how action-based intelligence can be an effective response to incidents*, Packt Publishing Ltd., 2018. Available: https://books.google.com/books?hl=en&lr=&id=jrZTDwAAQBAJ&oi=fnd&pg=PP1&dq=The+threat+detection+and+incident+response+processes+include+the+detection+of+potential+threats,+investigation+of+uncertainties,+elimination+of+root+causes+and+incorporation+of+actionable+measures+for+eliminating+potential+risks&ots=63aj6PIywy&sig=wrn2IvdhoC1heJpoaGtL0vNR34g.

[5] P. J. Sun, "Privacy protection and data security in cloud computing: a survey, challenges, and solutions," *IEEE Access*, vol. 7, pp. 147420-147452, 2019. Available: https://ieeexplore.ieee.org/abstract/document/8863330/

[6] U. M. Ismail and S. Islam, "A unified framework for cloud security transparency and audit," *J. Inf. Secur. Appl.*, vol. 54, p. 102594, 2020. Available: https://www.sciencedirect.com/science/article/pii/S2214212620307626.

[7] J. He et al., "Customized network security for cloud service," *IEEE Trans. Serv. Comput.*, vol. 13, no. 5, pp. 801-814, 2017. Available: https://ieeexplore.ieee.org/abstract/document/7974828/

[8] K. Spanaki, Z. Gürgüç, C. Mulligan, and E. Lupu, "Organizational cloud security and control: a proactive approach," *Inf. Technol. People*, vol. 32, no. 3, pp. 516-537, 2019. Available: https://www.emerald.com/insight/content/doi/10.1108/ITP-04-2017-0131/full/html.

[9] S. Loureiro, "Security misconfigurations and how to prevent them," *Netw. Secur.*, vol. 2021, no. 5, pp. 13-16, 2021. Available: https://www.magonlinelibrary.com/doi/abs/10.1016/S1353-4858%2821%2900053-2.

[10] B. Jin, S. Sahni, and A. Shevat, *Designing Web APIs: Building APIs That Developers Love*, O'Reilly Media, Inc., 2018. Available: https://books.google.com/books?hl=en&lr=&id=Dg1rDwAAQBAJ&oi=fnd&pg=PT6&dq=The+CSPs+offer+well-documented+APIs+for+providing+ease+of+customer+use,+despite+these+benefits,+they+pose+a+risk+to+property+security+&ots=VMGD08xSCd&sig=pOcdgDdmZUkuPJveu3ItYkwXJT0.

[11] S. Anson, *Applied incident response*, John Wiley & Sons, 2020. Available: https://books.google.com/books?hl=en&lr=&id=-jvKDwAAQBAJ&oi=fnd&pg=PR16&dq=he+threat+detection+process+focuses+on+the+collation+of+data+for+the+identification+of+emerging+threats+and+the+incident+responses+leverage+the+data+for+the+execution+of+the+remedial+actions.&ots=grzqg-JAqH&sig=-t1TGRH0PMFY19SSFN_QPouYn4g.

[12] S. Bhadra and S. Mohammed, "CLOUD COMPUTING THREATS AND RISKS: UNCERTAINTY AND UNCONROLLABILITY IN THE RISK SOCETY," *Electron. J.*, vol. 7, no. 2, pp. 1047-1071, 2020. Available: https://www.researchgate.net/profile/Research-Publication/publication/380543719_CLOUD_COMPUTING_THREATS_AND_RISKS_UNCERTAINTY_AND_UNCONROLLABILITY_IN_THE_RISK_SOCETY/links/6642ff977091b94e9326fceb/CLOUD-COMPUTING-THREATS-AND-RISKS-UNCERTAINTY-AND-UNCONROLLABILITY-IN-THE-RISK-SOCETY.pdf.

[13] A. Rath, B. Spasic, N. Boucart, and P. Thiran, "Security pattern for cloud SaaS: From system and data security to privacy case study in AWS and Azure," *Computers*, vol. 8, no. 2, p. 34, 2019. Available: https://www.mdpi.com/2073-431X/8/2/34.

[14] R. Yasrab, "Platform-as-a-service (paas): the next hype of cloud computing," *arXiv preprint arXiv:1804.10811*, 2018. Available: https://arxiv.org/abs/1804.10811.

[15] L. Reznik, *Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work for and Against Computer Security*, John Wiley & Sons, 2021. Available: https://books.google.com/books?hl=en&lr=&id=xZ1EEAAAQBAJ&oi=fnd&pg=PA9&dq=the+significance+of+artificial+intelligence,+machine+learning,+and+automation+holds+an+important+exertion+for+the+enhancement+of+threat+detection+abilities+&ots=oZmIg_Vx11&sig=dSDmqHAkMg3SWUaL32Afov-cOLQ.