ISSN: 2634 - 8853

Journal of Engineering and Applied Sciences Technology

SCIENTIFIC Research and Community

Review Article

Open Access

Cyber Resilience in Cloud-Based Critical Infrastructure

Pavan Nutalapati

USA

ABSTRACT

Cyber resilience within the cloud-based critical infrastructure refers to the capability of protecting electronic data and the systems from cyberattacks within the business operations within fintech sectors. The proposed research tries to investigate the cruciality of cyber resilience within cloud-based infrastructures. In the current era, the intense emergence of cyber threats necessitates the protection of critical infrastructure. The key findings of this research underline the dynamic approach to the maintenance of resilience against cyberattacks. Through providing actionable recommendations for the organizations, this research reinforces the baseline for the cloud security positions.

***Corresponding author**
Pavan Nutalapati, USA.

Received: February 02, 2023; **Accepted:** February 09, 2023; **Published:** February 20, 2023

Keywords: Cyber Resilience, Threat Detection, Cloud Security, AI-Driven Security, Advanced Persistent Threats, Critical Infrastructure

Introduction

In the present landscape of rapid digitalization, cyber-resilience within the cloud-based critical infrastructure becomes the foundation for organizations. Substantial integration of cloud technologies into the critical infrastructure including healthcare, financial, telecommunication and energy systems transforms itself with the alteration in sectoral strategies [1]. This further assists in the enhancement of flexibility, scalability and cost-effectiveness. The increasing emergence of various cyber threats such as data breaches, ransomware and other nation-state attacks necessitates the proper inclusion of cyber resilience within the cloud-based infrastructure.

Project Specification

This research study focused on the exploration of the main issues faced by organizations in the maintenance of data security and resilience within their cloud environments. It tries to highlight the importance of maintaining cyber resilience for cloud-based infrastructure through underlining the technological solutions and best practices that can mitigate these challenges.

Aims and Objectives

Aim

This research aims to evaluate the current state and importance of cyber resilience within the cloud-based critical infrastructure.

Objectives

- To address the key cyber threats to the cloud-based critical infrastructure
- To analyze the existing cyber resilience strategies within the cloud-based infrastructure
- To recommend potential improvement opportunities within the current practices

Research Questions

- What are the most emerging threats faced by the cloud-based critical infrastructure?
- What are the main gaps in the existing strategies and how can they be mitigated?
- How effective are the ongoing cyber resilience practices for eliminating these cyber threats?

Research Rationale

The rationale of this proposed research lies in ensuring cyber resilience within the cloud-based areas as cloud computing integrates rapidly with the operational activities of the critical infrastructure. Cyber resilience refers to a concept that assists businesses in fostering business continuity, organizational flexibility and information system security [2]. This research is persistent for the urgent requirement for strengthening the clou-based critical infrastructure against the emerging cyber threats.

Literature review

Research background

The increasing pace of digital transformation within critical infrastructure such as the energy grids, financial systems and healthcare services. The significance of this critical infrastructure relies substantially on scalability, cost-effectiveness and efficiency. Cybersecurity is necessary for the protection of digital assets through the inclusion of sensitive and personal financial information and intellectual property rights [3]. This research focuses on the exploration of the implementation of cyber resilience strategies in the cloud-based critical infrastructure. It substantially emphasises these strategies which can eliminate the risk level and enhance the overall security.

Critical assessment

Cyber resilience maintains the inventory of authorized and unauthorized devices and software. The development and management of protected configurations for all the devices. Despite the significant opportunities of cloud computing, the migration of the critical infrastructure to the cloud environments poses new issues that hinder the effectiveness of the cloud-based services. Traditional security techniques are often recognized as inadequate for the identification of dynamic threats [4]. Successful incorporation of the efficient cyber resilience system protects data security, prevents identity issues, protects intellectual property rights and mitigates business disruptions.

Linking with aim

This research aims to explore multifaceted aspects of cyber resilience within the cloud-based critical infrastructure. This proposed research focused on the development of a vigorous framework for the enhancement of cyber resilience within the cloud-based critical infrastructure. Through the critical analysis of the current practices, the proposition of the new strategies and the identification of potential gaps. The findings of this research provide insights for the policymakers, organizations and IT professionals who can able to foster the baseline for increasing infrastructural effectiveness.

Encapsulation of applications

This research tries to shed light on the importance of cyber security in the present landscape of cloud-based critical infrastructure. It also underlines the potential cyber threats within the ongoing digitalized era. The extracted insights of this research hold a wider application across the various sectors that rely on cloud-based critical infrastructure. For the fintech companies, the enhancement of the cyber resilience can be safeguarded against disruptions for the payment systems along with the financial markets.

Theoretical framework

There exist various theories related to cyber resilience in cloud-based critical infrastructure. Abdullayeva (2023) highlights various theories that align with the proposed research topic. The resilience engineering theory focuses on the significance of resilience engineering within intelligent cloud computing systems. The focal point of this theory is the design of systems that can adapt the vigorous measures from unexpected challenges [5]. The "Complicated Adaptive Systems" theory considers the intelligent cloud system as the dynamic components that consist of interactive elements for the alteration of this environment [6]. Within the critical infrastructure, this theory recommended that the cloud-based systems have to be structured for the adoption of autonomous cyber threats and increase resilience.

Literature gap

There exists vast varied enriched literature that researches cybersecurity within the cloud environments within the critical infrastructure. However, a significant lack is visible in the development of a comprehensive framework that identifies the arisen challenges of cyber resilience. A maximum number of studies focused on security without focusing on the actual concepts of various security threats.

Methodology

Research Philosophy

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 emerging cyber threats. This philosophy assists in the exploration of human behaviour in response to cyber-attacks and understanding the reliable and consistent measures for the mitigation of these threats.

Research Approach

In order to conduct the overall research, this paper employed a deductive research approach which assists in the exploration of the potential cyber threats through using various theories. Utilization of this research approach helps the researchers to generalize their ideas and then test these through the incorporation of specific observations.

Research design

The qualitative research design is incorporated in this research for the specification of qualitative insights about cyber resilience within the cloud-based critical infrastructure. This research design analyses the scenario-based methodology which highlights the diverse range of threats and various types of vulnerabilities for delivering answers to the research questions.

Data collection method

The peer review data collection method is used in this research to elaborately discuss the actual contents of different literature, articles and journals. The peer-review process assists in ensuring that the used articles and journals provide verifiable, accurate and valuable contributions to the proposed field of study. It also contributes to the prevention of personal biases from affecting the outcomes of various threat-eliminating measures within cloud computing settings.

Ethical consideration

The ethical consideration for the study related to the analysis of cyber resilience includes the maintenance of fairness, data privacy, accountability and transparency within the handling of data [7]. It ensures the implementation of the vigorous security measures and response to the threats as well. This research paper focused on the maintenance of privacy along with the confidentiality of the information. It focuses on the avoidance of data misuse by using the ethical principles that help to prevent misuse of the data for manipulative and exploitative purposes.

Results

Critical analysis

Cyber resilience refers to an emerging security paradigm that promotes a vigorous and dynamic approach to securing organizational information. Within the evolving landscape of cybersecurity, organizations are required to incorporate more resilient and persistent cyber strategies to deal with cyber threats. The cyber resilience techniques rely on the five key pillars including identity, protection, threat detection, response and recovery [8].

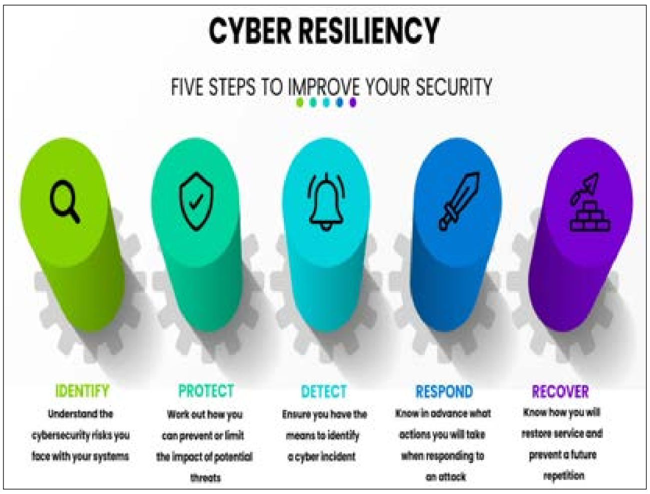
CYBER RESILIENCY
FIVE STEPS TO IMPROVE YOUR SECURITY
IDENTIFY
Understand the cybersecurity risks you face with your systems
PROTECT
Work out how you can prevent or limit the impact of potential threats
DETECT
Ensure you have the means to identify a cyber incident
RESPOND
Know in advance what actions you will take when responding to an attack
RECOVER
Know how you will restore service and prevent a future repetition

Figure 1: Cyber Resilience Infrastructure [8]

The cyber-resilient infrastructure is safeguarded against cyber threats and ensures continuous operation. This further assists in the minimisation of the risks and service disruption.

Findings and Discussion

Theme 1: key cyber threats to the cloud-based critical infrastructure

The cloud-based critical infrastructure poses several issues in the existing cyber security systems. One of the most crucial issues in cyber security for critical infrastructure is the widespread utilisation of the legacy system [9]. The traditional systems are inadequate to prevent cyber threats resulting in issues in identifying and targeting the cyber criminals. Insider threats are the emerging risks for critical infrastructure in case of both accidental and international threats. Ransomware attacks are a commonly spread incident with 214 incidents in the first quarter of 2023 which increase of 13 per cent from the previous quarter [10]. In case of the financial technology-based companies, the increasing emergence of advanced persistent threats steals the data and maintains extended access to the cyber security systems. The distributed denial of services attacks the critical infrastructure systems with traffic which causes significant disruption in various areas, especially financial and technology-based sectors. Artificial intelligence expedites these cyber-attacks by reducing the average speed of the DDoS from 184 seconds in 2021 to only 55 seconds in 2022.

Theme 2: Existing cyber resilience strategies within the cloud-based infrastructure

The cyber resilience strategies aligned with the organizational objectives through the identification of the current information, services and systems which are essential for the organizations. The holistic cyber resilience strategy includes cybersecurity at all levels to safeguard the organizations through detecting threats and recovering from the issues. The cyber resilience strategy includes cybersecurity systems that assist in the protection of systems, data and applications [11]. Preventing the hostile issues through the identification of potential vulnerabilities is necessary for securing cloud infrastructures from the sticking effects. It includes the endpoint detection and responses along with the extended detection and responses. Despite the vigorous cybersecurity measures, the risk of cyber-based incidents poses significant issues which have to be maintained through proposing business continuity and resilience programmes. In the case of the efficiency process and technology, the initiatives regarding cyber resilience and string governance become paramount for the organizations. It assists substantially in the maintenance of people's activity, process and actionable solutions for providing guidance to cyber resilience.

Theme 3: potential improvement opportunities within the current practices

In order to keep the organization cyber-safe, the organizations have to focus on some key techniques. It is essential for organisations to determine the possible events of a cyber incident, through the identification of the essential information, the cyber security techniques expand the baseline for the cyber-resilience strategy.

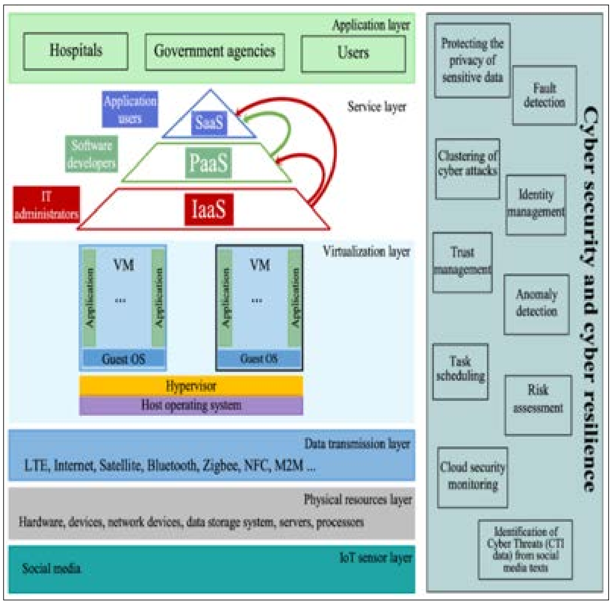

Figure 2: Cyber Security Reference Model [13]

The technological aspects are not enough for the elimination of cyber vulnerabilities. The significant integration of cyber-resilience mechanisms through ensuring the skills of the employees contributes significantly in the protection drawing any security incident. Organizations should increase the investment level in the stimulation of "Security Information and Event Management" is crucial for maintaining the scalability and consistency within the cloud-based critical infrastructure.

Evaluation

The field of this research is grounded in the potential issues related to the cyber securities. This research focuses on the evaluation of the efficiency of present cyber-resilient strategies for the protection of the operational activities within the fintech sector. This research paper underlines the growing requirement of strengthening cloud-based systems against emerging cyber threats such as advanced persistent threats and ransomware. The evaluation shows that the continual risk of cyber incidents necessitates ongoing improvement within the resilient measures. The incorporation of effective cyber-threat mitigation techniques expands the way for vigorous maintenance of cyber threats and coordination between various cyber security techniques. IT further contributes to the protection and enhancement of security within critical infrastructure in the digital regime.

Conclusion

In conclusion, it can be said that the research on cyber resilience in cloud-based critical infrastructure underlines the essentiality of vigorous security frameworks for the protection against cyber threats. The proposed study showcases that the integration of advanced threat detection and the real-time monitoring of the cloud architecture significantly enhances the prevention mechanisms of the critical infrastructure. The dynamic nature of the cyber threats and technical vulnerabilities expands the requirements for the continuous evolution of the strategies. This research contributes to the knowledge and practical insights for protecting essential services in the increasingly digital landscape.

Research Recommendation

The recommendation of this research relies on the management of the critical infrastructure for the adoption of dynamic measures for cyber resilience. The inclusion of leveraged AI-driven threat detection and the adoption of the zero-trust architectures. The collaboration among government bodies and security professionals is essential for the development of standardized practices for the protection of critical infrastructure. In addition to this, regular flexibility testing through the incorporation of penetration testing for the identification of potential vulnerabilities.

Future Work

Future research in this area has to focus on the development of adaptive security systems that assist in the detection, analysis and mitigation of the growing threats in the present phenomenon. The exploration of the integration of quantum computing, artificial intelligence, blockchain technology and machine learning for the enhancement of data integrity within the cloud environments. Future research has to examine the social-technical prospects of cyber resilience. The special focus has to be on the influence of human factors on the effectiveness of security measures. In addition to this, the comparative analysis of the diverse range of cloud platforms in the area of resilience and efficiency of security [14-39].

References

1. Kumar, Sharma S, Singh A, Alwadain A, Choi BJ, et al. (2021) Revolutionary strategies analysis and proposed system for future infrastructure in internet of things. Sustainability 14: 71.
2. Annarelli, Nonino F, Palombi G (2020) Understanding the management of cyber resilient systems. Comput. Ind. Eng 149: 106829.
3. Chaisse J, Bauer C (2018) Cybersecurity and the protection of digital assets: assessing the role of international investment law and arbitration. Vand. J. Ent. & Tech. L 21: 549.
4. Manulis M, Bridges CP, Harrison R, Sekar V, Davis A (2021) Cyber security in new space: analysis of threats, key enabling technologies and challenges. Int. J. Inf. Secur 20: 287-311.
5. Arbaoui, Yusraw O, Yuso P, Hareebin Y (2022) An Agent-Based Model for Situational Awareness at Workplace. Int. J. Intell. Eng. Syst 15: 5.
6. Wylde V, Rawindaran N, Lawrence J, Balasubramanian R, Prakash E, et al. (2022) Cybersecurity, data privacy and blockchain: A review. SN Comput. Sci 3: 127.
7. Amdhservicesltd.com, Five steps to improve cyber resilience.
8. Lehto M (2022) Cyber-attacks against critical infrastructure. in Cyber Security: Critical Infrastructure Protection, Cham: Springer International Publishing 3-42.
9. Trautman LJ, Shackelford S, Elzweig B, Ormerod P (2022) Cyber Threats to Business: Identifying and Responding to Digital Attacks. Northern Illinois Univ. Coll. Law Legal Stud. Res. Paper No. Forthcoming.
10. Petrenko S (2022) Cyber resilience. River Publishers https://www.riverpublishers.com/flyer_pdf/create_flyer_new.php?id=731
11. Dupont (2019) The cyber-resilience of financial institutions: significance and applicability. J. Cybersecurity 5: tyz013.
12. Lo WW, Layeghy S, Sarhan M, Gallagher M, Portmann M (2022) E-graphsage: A graph neural network based intrusion detection system for IoT. in Proc. 2022 IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS) pp1-9.
13. Kok H, Weijters G, Numan P, Voorveld A (2020) Resilience of Critical Infrastructure Against Cyber Threats. in Cyber Security in Critical Infrastructures: State of the Art and Prospects. Cham: Springer pp1-28.
14. Ross R, Pillitteri V, Graubart R, Swanson A (2019) Developing Cyber Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 2: 800-160.
15. Haimes YY (2019) Models for risk management of systems of systems. in Handbook of Systems Engineering and Management, 2nd ed. Hoboken, NJ, USA: Wiley 1-34.
16. Smith MT, Ibrahim AI, Dolan PJ (2019) Achieving Cyber Resilience in Mission Critical Systems. IEEE Security & Privacy 17: 24-33.
17. Ramana MV (2021) Cybersecurity in nuclear power plants: Insights from a systems engineering perspective. Bulletin of the Atomic Scientists 77: 1-9.
18. Gruschka N, Jensen M, Iacono LL, Luttenberger N (2021) An analysis of the cloud computing security problem. in Proc. 2021 IEEE International Conference on Cloud Computing (CLOUD) pp1-8.
19. Sivabalan, Lee J, Teague KA, Krishnan KR (2021) Security in Cloud-Based Critical Infrastructure: Challenges and Solutions. IEEE Access 9: 1-15.
20. Cardenas, Manadhata PK, Rajan S (2017) Big Data Analytics for Security Intelligence. IBM Journal of Research and Development 61: 1-10.
21. Holz, Steiner M, Dahl F, Biersack E, Freiling F (2008) Measurements and mitigation of peer-to-peer-based botnets: A case study on StormWorm. in Proc. 2008 Annual Computer Security Applications Conf pp141-150.
22. Zhuang C, Abhishek A, Manadhata P (2019) Understanding Security Issues in Cloud-Based Internet of Things. in Proc. 2019 IEEE/ACM Symposium on Edge Computing (SEC) pp1-8.
23. Mailloux JJ, Demirel TH, Thomas RW (2020) Quantum Computing and Its Implications on Cybersecurity. Military Cyber Affairs 6: 1-9.
24. Bhimani KR (2020) Critical Infrastructure and the Challenges of Cyber Resilience. Journal of Cyber Policy 5: 1-15.
25. Easwaran NA, Rajarathnam M (2019) A Survey on Cybersecurity Challenges in Cloud Computing. Procedia Computer Science 87: 1-8.
26. Nissenbaum H (2018) Cybersecurity and privacy: The new challenges. Daedalus, 140: 1-13.
27. Dasgupta, Wang LF, Gu Q (2019) A Hybrid Framework for Cyber Defense. Future Generation Computer Systems 92: 1-14.
28. Dumont B (2017) Building a Secure and Resilient IoT. in Handbook of System Safety and Security, 1st ed., Boston: Syngress pp 1-18.
29. Ma W, Abazari MM, Hwang K, Li W (2020) Cybersecurity Strategies for Cloud Computing Networks. IEEE Internet of Things Journal 7: 1-10.
30. Somani, Gaur M (2016) Defending against Distributed Denial of Service in Cloud Computing Using Trust Management. IEEE Transactions on Dependable and Secure Computing 13: 1-12.
31. Chiu DK, Lam KK (2018) Secure Data Management and Applications in Cloud Computing. Computing, 100: 1-12.
32. Shabut, Lwin M, Hossain S (2019) Risk Assessment in Cloud Computing and Cyber Resilience in Cloud Services. in Proc. 2019 8th International Conference on Emerging Security Technologies (EST) pp1-8.
33. Pathan K (2019) The State of Cybersecurity in IoT Ecosystems: A Survey. Journal of Network and Computer Applications 143: 1-12.

34. Gentry P (2019) Blockchain Technology and Its Impact on Cybersecurity in Cloud-Based Systems. Journal of Cyber Policy 4: 1-12.
35. Bernstein DJ, Lange T (2018) Post-Quantum Cryptography: Current State and Future Directions. IEEE Security & Privacy 16: 1-9.
36. Johnson W (2019) The Role of Cybersecurity in Ensuring the Reliability of Cloud Services. Reliability Engineering & System Safety 189: 1-9.
37. Gupta NPS (2020) Artificial Intelligence in Cybersecurity: Emerging Threats and Opportunities. Future Generation Computer Systems 113: 1-10.
38. Calo SB (2018) Privacy and Cybersecurity in the Internet of Things (IoT). Computer Law & Security Review 34: 1-13.
39. Chen TM, Sehra S (2019) The Future of Cybersecurity: Challenges and Emerging Trends. Journal of Information Security and Applications 44: 1-12.

Copyright:© 2023 Pavan Nutalapati. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.