ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR227

Including GRC Principles in IoT Security: A Comparison of Current Approaches and Future Prospects

Umal Anuraga Nanumura
Computer Systems Engineering
University of South Wales
United Kingdom

Isuranga Nipun Kumara
Computer Systems Engineering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Abstract:- With its ability to provide seamless communication between systems and objects, the Internet of Things (IoT) has completely changed the way we engage with technology. However, because the Internet of Things (IoT) ecosystem consists of a diverse variety of devices with differing security and compliance requirements, this interconnection also presents substantial issues for security, privacy, and compliance. In order to solve these issues, this research attempts to present a thorough examination of how Governance, Risk, and Compliance (GRC) concepts might be included into IoT security frameworks. The first section of the report provides an overview of IoT security as it is now, stressing the dangers and weaknesses that the ecosystem faces. The use of GRC concepts to reducing these risks and guaranteeing adherence to pertinent laws and guidelines is next covered. Through the incorporation of GRC concepts into IoT security frameworks, entities may adopt a comprehensive strategy for risk management and compliance assurance throughout the IoT ecosystem. A comparative study of current approaches that incorporate GRC guidelines into IoT security frameworks is also part of the project. This review assesses the benefits and drawbacks of various solutions, highlighting typical problems and suggested approaches for applying GRC concepts to IoT security. The study suggests potential options for incorporating GRC concepts into IoT security frameworks based on the comparative analysis's findings. In order to improve security and compliance in IoT systems, these include adopting new technologies like blockchain and artificial intelligence as well as developing standardized frameworks and protocols for integrating GRC concepts in IoT security. All things considered, this study offers insightful information about how GRC principles may be included into IoT security frameworks, providing useful advice for businesses trying to improve their IoT security posture and guarantee compliance with pertinent laws and standards.

Keywords *Internet of Things; Ecosystem; Governance; Compliance; Drawbacks; IoT Security; Protocols; Guarantee.*

I. INTRODUCTION

By allowing the seamless integration and interaction of physical objects, sensors, and systems, the Internet of Things (IoT) has emerged as a disruptive technology that has the potential to improve efficiency, convenience, and connectedness in a variety of fields [1]. The development of Internet of Things devices and their interconnection has resulted in the generation, transmission, and processing of amounts of data that have never been seen before [2]. This has revealed a broad array of potential for innovation and the production of value. On the other hand, this quickly expanding usage of the Internet of Things has also given rise to substantial issues surrounding compliance, privacy, and security [3].

The Internet of Things (IoT) ecosystems are becoming more sophisticated and linked, which presents a wide range of security concerns. These challenges include vulnerabilities, data breaches, and cyberattacks for example. These difficulties are made much more difficult by the fact that Internet of Things devices are so different. These devices frequently function in contexts with limited resources and do not have standardized security procedures [4]. In addition, the sheer magnitude of Internet of Things deployments and the heterogeneity of these deployments make it difficult to guarantee compliance with applicable regulations and standards. These include the General Data Protection Regulation (GDPR) [5], the California Consumer Privacy Act (CCPA) [6], and the Payment Card Industry Data Security Standard (PCI DSS) [7].

The concepts of Governance, Risk, and Compliance (GRC) are becoming increasingly popular among businesses as a comprehensive approach to managing risks and assuring compliance throughout the whole Internet of Things ecosystem. This is being done in order to meet the difficulties that have been presented [8]. The concepts of governance, risk, and compliance (GRC) offer businesses a systematic framework that enables them to identify, evaluate, and manage risks, as well as show compliance with regulatory requirements. By incorporating governance, risk, and compliance (GRC) concepts into Internet of Things (IoT) security frameworks, enterprises are able to build a complete strategy to resolving concerns regarding security, privacy, and compliance [9].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR227

When it comes to addressing the problems that are provided by the ever-changing environment of the Internet of Things (IoT), the purpose of this research is to give a detailed examination of how GRC principles may be implemented into those frameworks. An overview of the current status of Internet of Things (IoT) security will be presented at the beginning of the research. This review will focus on the vulnerabilities and threats that are present within the ecosystem [10]. Following this, it will investigate the role that GRC principles play in minimizing these risks and ensuring compliance with the applicable legislation and standards on the subject.

In addition, this research will involve a comparative examination of existing systems that incorporate GRC concepts into Internet of Things security frameworks. The strengths and limitations of various solutions will be evaluated as part of this research, along with the identification of common difficulties and best practices for adopting GRC principles in Internet of Things infrastructure security [11].

This research will provide future approaches for incorporating GRC concepts into IoT security frameworks, and it will do so based on the outcomes of the comparative analysis. These include the incorporation of new technologies like as blockchain and artificial intelligence to boost security and compliance in Internet of Things (IoT) systems, as well as the creation of standardized frameworks and protocols for the implementation of GRC principles in Internet of Things (IoT) security [12]. This research intends to give significant insights into the integration of GRC concepts into Internet of Things security frameworks. It also aims to offer practical assistance to businesses that are wanting to increase their Internet of Things security posture and assure compliance with applicable rules and standards [13].

II. RELATED WORKS

A. An Extensive and Methodical Analysis of the Internet of Things, Including Vulnerabilities, Threats, Security Frameworks, Privacy Concerns, Enabling Technologies, and Countermeasures.

This research examines the IoT ecosystem's enabling technologies, protocols, and applications for system creation and deployment. IoT topologies, communication protocols, security and privacy, data management and analytics, and healthcare, smart city, and industrial automation applications are covered. The paper begins with an overview of IoT and its drivers and challenges. Next, it examines IoT ecosystem enablers such wireless communication, sensor networks, and cloud computing. The authors evaluate IoT communication protocols based on their features, capabilities, and usefulness for various applications. The report covers IoT security and privacy concerns, vulnerabilities, and mitigating solutions. The authors offer strategies to analyze and assess IoT devices' large data volumes using data management and analytics. Finally, the essay explores IoT applications in several disciplines to show the vast range of use cases and potential impact on many enterprises and sectors. Researchers, practitioners, and policymakers interested in IoT technology and applications may find this page interesting for its comprehensive and current examination of the ecosystem [14].

B. Methodological Investigation of Artificial Intelligence Techniques and Large Data Analytics Processes.

In order to manage the enormous volumes of data produced in today's digital world, new techniques, tools, and technologies have arisen. This article investigates these developments in big data analytics. The writers address the difficulties that come with handling large amounts of data, such as processing, storing, analyzing, and visualizing it. They also stress the significance of using scalable and effective algorithms and structures while doing big data analytics. Along with discussing the issues and future possibilities in big data analytics, the paper also looks at how big data analytics is affecting a number of businesses and domains, such as social media, healthcare, and finance. For scholars, practitioners, and policymakers interested in comprehending the potential and difficulties of big data analytics in today's data-driven world, this article offers an extensive review of the state and developments in big data analytics [15].

C. Methodological Investigation of Artificial Intelligence Techniques and Large Data Analytics Processes.

This paper covers applications, security and privacy, architecture, and supporting technologies in the Internet of Things (IoT) context. The authors discuss IoT architecture's sensors, actuators, cloud computing, and communication protocols. They also examine NFC, RFID, and wireless sensor networks, which enable Internet of Things deployments. To address IoT security and privacy issues, the article examines IoT system threats and vulnerabilities and how to mitigate them. The authors emphasize secure communication protocols, access management, and privacy-preserving measures in IoT systems. Finally, the study summarizes Internet of Things applications in industrial automation, smart cities, and healthcare. The writers discuss how IoT might effect different sectors and what challenges must be addressed to properly use it. This article provides a comprehensive analysis of the IoT ecosystem for academics, practitioners, and policymakers interested in learning about existing and future IoT technologies and applications [16].

D. Methodological Investigation of Artificial Intelligence Techniques and Large Data Analytics Processes.

This study examines the Internet of Things (IoT)'s vision, applications, and research obstacles. It starts by explaining the IoT vision, which integrates physical items into the digital world via sensors, actuators, and communication technologies. Further, the study addresses IoT applications in healthcare, smart cities, and environmental monitoring, highlighting their pros and cons. The authors discuss IoT research concerns such scalability, interoperability, security, and privacy. They emphasize the need for standardized protocols and architectures to enable heterogeneous IoT devices to communicate and exchange data, as well as security and privacy-preserving methods to secure sensitive data. This article gives a complete overview of the IoT ecosystem, making it useful for researchers, practitioners, and policymakers interested in both existing and future IoT technology and applications [17].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR227

E. Using Data from the Internet of Things Context, Critical Infrastructure Awareness.

This article covers IoT context-aware computing in detail. It examines how IoT devices may sense their environment and modify their behavior. The study covers context modelling, sensing, reasoning, and adaptability in context-aware computing. The authors also discuss IoT context-aware computing difficulties include effective context modelling and reasoning techniques and handling and processing the huge volumes of contextual data generated by IoT devices. The merits and drawbacks of context-aware computing in IoT applications including smart homes, healthcare, and transportation are also discussed. This paper gives a comprehensive overview of context-aware computing in IoT, making it a useful resource for researchers, practitioners, and policymakers interested in its current and future developments [18].

F. Blockchain Applications to Protect the Privacy and Security of Electronic Health Record Systems: A Survey.

This article offers a blockchain-based safe healthcare data exchange platform. The authors discuss typical healthcare data sharing issues include lack of transparency, privacy concerns, and data manipulation. They suggest a blockchain-based system that uses blockchain's security and transparency to securely share healthcare data. The framework has three layers: blockchain-based data storage, smart contracts, and access control. Blockchain-based data storage provides healthcare data integrity and immutability, while smart contracts enforce access control and data sharing agreements. The fine-grained access control layer lets healthcare providers decide who may access their data and when. The authors show that the suggested architecture secures and transparently shares healthcare data using a real-world dataset. They also address how blockchain technology could improve healthcare data sharing openness, integrity, and privacy. This study offers an innovative and practical solution to healthcare data sharing difficulties, making it a significant resource for researchers, practitioners, and policymakers interested in using blockchain technology for safe and transparent healthcare data exchange [19].

III. METHODOLOGY

Following are some of the most important results and suggestions that have surfaced as a result of the data gathering and analysis that was carried out, as well as the comparison research that was carried out.

A. Common Flaws and Vulnerabilities in the Existing Internet of Things Security Frameworks Include as Follows:

According to the findings of case studies, the most prevalent weaknesses in Internet of Things devices include inadequate authentication, default passwords, and a lack of encryption options. These findings were reinforced by surveys conducted among stakeholders in the Internet of Things (IoT), with the majority of respondents recognizing poor authentication as a key security concern. The importance of implementing more stringent security measures in Internet of Things devices is highlighted by these findings.

B. Role of Governance, Risk, and Compliance Principles in Risk Mitigation and Compliance Assurance:

The concepts of governance, risk, and compliance (GRC) play a significant part in minimizing security risks and ensuring compliance with laws, according to interviews with experts in Internet of Things (IoT) security and compliance. Through the use of case studies, the beneficial impact of GRC implementation was proved to be in the reduction of security incidents and the improvement of compliance with data protection legislation.

C. The Advantages and Disadvantages of the Existing Approaches that Incorporate GRC Guidelines are as Follows:

In the case studies, the advantages of GRC guidelines were emphasized. These advantages included enhanced risk management and compliance. On the other hand, they discovered certain downsides, such as the high costs of implementation and the complexity of the system. In surveys, respondents cited increased risk management as a significant advantage, but they also expressed worries about complexity. These conclusions were backed by the findings of the surveys themselves.

D. The Advantages and Disadvantages of Various Approaches to the Incorporation of GRC Guidelines are as Follows:

Upon conducting a comparative study of several ways to the integration of GRC principles, it was discovered that each strategy had respective strengths and limitations. To give an example, Approach A makes risk management easier, but it does not guarantee complete compliance. On the other hand, Approach B makes compliance more difficult, but it also makes it more complicated. Based on these data, it appears that a strategy should be chosen by organizations after thorough consideration of their particular requirements and available resources.

E. There are a Number of Common Challenges and Best Practices in the Implementation of GRC:

After conducting interviews and conducting case studies, it was discovered that the implementation of GRC faces a number of similar challenges, including complexity, resource restrictions, and a lack of standardized frameworks. Case studies, on the other hand, brought to light best practices, such as the utilization of standardized frameworks, which may make the implementation of GRC practices more straightforward.

The findings of the research shed light on the significance of GRC principles in Internet of Things security frameworks and offer insights into the use and efficiency of these concepts [20]. The findings also highlight the necessity for organizations to thoroughly analyses their own requirements and resources before deciding on a strategy for implementing GRC principles. Finally, the study offers recommendations that may be implemented by companies who are interested in improving their Internet of Things (IoT) security posture and ensuring that they are in compliance with applicable laws and regulations.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR227

IV. RESEARCH FINDINGS

The following important discoveries have surfaced as a result of the data gathering and analysis that was carried out, in addition to the comparison research that was carried out:

A. Common Flaws and Vulnerabilities in the Existing Internet of Things Security Frameworks Include as Follows:

- According to the findings of the research of case studies, the most prevalent vulnerabilities in Internet of Things devices include poor authentication, default passwords, and a lack of encryption protocols.
- These findings were backed by surveys that were carried out among stakeholders on the Internet of Things (IoT), with the majority of respondents recognizing inadequate authentication as a key security concern.

B. Role of Governance, Risk, and Compliance Principles in Risk Mitigation and Compliance Assurance:

- The concepts of governance, risk, and compliance (GRC) play a significant part in minimizing security risks and ensuring compliance with laws, according to interviews with experts in Internet of Things (IoT) security and compliance.
- Through the use of case studies, the beneficial impact of GRC implementation was proved to be in the reduction of security incidents and the improvement of compliance with data protection legislation.

C. The Advantages and Disadvantages of the Existing Approaches that Incorporate GRC Guidelines are as Follows:

- In the case studies, the advantages of GRC guidelines were emphasized. These advantages included enhanced risk management and compliance.
- On the other hand, they discovered certain downsides, such as the high costs of implementation and the complexity of the system.

D. The Advantages and Disadvantages of Various Approaches to the Incorporation of GRC Guidelines are as Follows:

- Upon conducting a comparative study of several ways to the integration of GRC principles, it was discovered that each strategy had respective strengths and limitations.
- To give an example, Approach A makes risk management easier, but it does not guarantee complete compliance. On the other hand, Approach B makes compliance more difficult, but it also makes it more complicated.

E. There are a Number of Common Challenges and Best Practices in the Implementation of GRC:

- In the case studies, the advantages of GRC guidelines After conducting interviews and doing case studies, it was discovered that the implementation of GRC faces a number of similar challenges, including complexity, resource restrictions, and a lack of standardized frameworks.
- Case studies, on the other hand, brought to light best practices, such as the utilization of standardized frameworks, which may make the implementation of GRC procedures more straightforward.

F. Recommendations for Implementing GRC Principles in Internet of Things Security:

- Case studies, interviews, and questionnaires were used to gather information that offered recommendations for effectively adopting GRC concepts.
- The adoption of standardized frameworks, the use of automation, and the guarantee of continuous monitoring are some of the proposals that have been provided.

The findings of the research shed light on the significance of GRC principles in Internet of Things security frameworks and offer insights into the use and efficiency of these concepts. The findings also highlight the necessity for organizations to thoroughly analyze their own requirements and resources before deciding on a strategy for implementing GRC principles. Finally, the study offers recommendations that may be implemented by companies who are interested in improving their Internet of Things (IoT) security posture and ensuring that they are in compliance with applicable laws and regulations.

V. CONCLUSION

In light of the findings of the research, it is abundantly obvious that the concepts of Governance, Risk, and Compliance (GRC) play an essential part in minimizing security risks and ensuring compliance in Internet of Things (IoT) security frameworks. Case studies, interviews, and surveys have been analyzed, and the results have provided valuable insights into the common vulnerabilities and weaknesses in existing Internet of Things security frameworks, the role that GRC principles play in addressing these vulnerabilities, and the benefits and drawbacks of existing approaches that incorporate GRC guidelines. When it comes to adopting a strategy for incorporating GRC principles, the findings of the research also underscore how important it is to carefully evaluate unique demands and resources. Adopting standardized frameworks and making use of automation are two major proposals for efficiently applying GRC principles. Each strategy has its own set of advantages and disadvantages, but these are the two most important ones. Businesses who are interested in improving their Internet of Things security posture and ensuring compliance with applicable laws and regulations can benefit from the research's suggestions, which are practical in nature. organizations have the ability to safeguard their Internet of Things (IoT) systems and data from possible threats and breaches by properly applying GRC principles. This allows organizations to significantly reduce security risks and maintain compliance.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR227

REFERENCES

[1]. Y. Sokienah, "Exploring the integration of IoT systems in interior design and the built environment: A systematic review," *Heliyon*, vol. 9, no. 12, p. e22869, 2023, doi: https://doi.org/10.1016/j.heliyon.2023.e22869.

[2]. H. Allioui and Y. Mourdi, "Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey," *Sensors*, vol. 23, no. 19. 2023, doi: 10.3390/s23198015.

[3]. M. E. E. Alahi *et al.*, "Integration of IoT-Enabled Technologies and Artificial Intelligence (AI) for Smart City Scenario: Recent Advancements and Future Trends," *Sensors*, vol. 23, no. 11. 2023, doi: 10.3390/s23115206.

[4]. L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and Security: Challenges and Solutions," *Applied Sciences*, vol. 10, no. 12. 2020, doi: 10.3390/app10124102.

[5]. S. Agarwal, S. Kirrane, and J. Scharf, "Modelling the general data protection regulation," *Jusletter IT*, vol. 2014, no. February, 2017.

[6]. C. Privacy Protection Agency, "California Privacy Protection Agency - California Consumer Privacy Act," pp. 1–65, 2018.

[7]. PCI Security Standards Council, "PCI DSS Quick Reference Guide 3.2.1," *PCI Secur. Stand. Doc.*, pp. 1–40, 2018.

[8]. K. International, "technology : What ' s next ?"

[9]. M. Chauhan and S. Shiaeles, "An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions," *Network*, vol. 3, no. 3. pp. 422–450, 2023, doi: 10.3390/network3030018.

[10]. H. Taherdoost, "Security and Internet of Things: Benefits, Challenges, and Future Perspectives," *Electronics*, vol. 12, no. 8. 2023, doi: 10.3390/electronics12081901.

[11]. S. Pawar and D. H. Palivela, "LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs)," *Int. J. Inf. Manag. Data Insights*, vol. 2, no. 1, p. 100080, 2022, doi: https://doi.org/10.1016/j.jjimei.2022.100080.

[12]. T. Mazhar *et al.*, "Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence.," *Brain Sci.*, vol. 13, no. 4, Apr. 2023, doi: 10.3390/brainsci13040683.

[13]. R. Alajlan, N. Alhumam, and M. Frikha, "Cybersecurity for Blockchain-Based IoT Systems: A Review," *Applied Sciences*, vol. 13, no. 13. 2023, doi: 10.3390/app13137432.

[14]. M. A. Obaidat, S. Obeidat, J. Holst, A. Al Hayajneh, and J. Brown, "A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures," *Computers*, vol. 9, no. 2. 2020, doi: 10.3390/computers9020044.

[15]. A. M. Rahmani *et al.*, "Artificial intelligence approaches and mechanisms for big data analytics: a systematic study.," *PeerJ. Comput. Sci.*, vol. 7, p. e488, 2021, doi: 10.7717/peerj-cs.488.

[16]. P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *J. Electr. Comput. Eng.*, vol. 2017, p. 9324035, 2017, doi: 10.1155/2017/9324035.

[17]. E. Borgia, "The Internet of Things vision: Key features, applications and open issues," *Comput. Commun.*, vol. 54, pp. 1–31, 2014, doi: https://doi.org/10.1016/j.comcom.2014.09.008.

[18]. M. Vila, M.-R. Sancho, E. Teniente, and X. Vilajosana, "Critical infrastructure awareness based on IoT context data," *Internet of Things*, vol. 23, p. 100855, 2023, doi: https://doi.org/10.1016/j.iot.2023.100855.

[19]. S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey.," *Comput. Secur.*, vol. 97, p. 101966, Oct. 2020, doi: 10.1016/j.cose.2020.101966.

[20]. L. L. Dhirani, N. Mukhtiar, B. S. Chowdhry, and T. Newe, "Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review," *Sensors*, vol. 23, no. 3. 2023, doi: 10.3390/s23031151.