The 1st International Student Conference on Economics and Business Excellence (ISCEBE) 2024
e-ISSN: xxxx-xxxx/Vol. 1 No. 1 (2024)

FROM RISK TO RESILIENCE: A SYSTEMATIC REVIEW OF APPLICATION SYSTEM SECURITY CONTROLS AND RISK MANAGEMENT

Kevry Ramdany[1)], Asniati Bahari[2)]
[1,2)]Management Study Program, Universitas Andalas, Indonesia
Corresponding author: asniati@eb.unand.ac.id

Abstract

This study reviews the evolving challenges in the application of security controls and risk management strategies for application systems, specifically focusing on the transition from risk mitigation to resilience. As organizations increasingly rely on digital systems for critical business operations, the security of these systems becomes paramount. Cyber threats such as ransomware, data breaches, and system vulnerabilities are escalating, impacting financial and operational stability. This paper systematically reviews recent literature (2020-2024) to identify trends, effective security controls, and best practices in managing application system risks. The findings suggest that while technologies like multi-factor authentication, encryption, and intrusion detection are vital, many organizations still fail to manage risks effectively. The study highlights the importance of resilience, emphasizing proactive risk assessment and system fortification to not only withstand but recover quickly from cyberattacks. Using a systematic review methodology (PRISMA), this paper synthesizes key empirical evidence to offer organizations actionable insights for enhancing application system security and resilience in the face of evolving cyber threats.

Keywords: Application System Security, Risk Management, Cyber Resilience, Security Controls, and Systematic Review

Introduction

In this rapidly developing digital era, application systems have become the operational backbone of many organizations, from the commercial sector to government. These systems are used to support various critical business functions, including financial transactions, customer management, and sensitive data processing. However, along with the increasing dependence on information technology, various threats have emerged that directly affect the security and safety of application systems. These threats include cyberattacks, data breaches, misconfigurations, and weaknesses in application architecture that can lead to operational failures or economic losses (Deloitte, 2021).

According to research from Kaspersky (2020), cyberattacks on application systems have increased sharply in recent years, especially in the form of ransomware attacks, exploitation of application vulnerabilities, and data theft. Those without adequate security controls are at high risk of facing significant security incidents. In fact, according to a report from IBM Security (2021), the average cost of a data breach reached $4.24 million in 2021, with most breaches occurring through application vulnerabilities.

Risk management is an important approach to mitigate these vulnerabilities. Organizations need to implement a robust and ongoing security control approach to protect their application systems from both internal and external threats. These security controls include mechanisms such as multifactor authentication, data encryption, continuous monitoring, and intrusion detection systems (IDS). Several standards, such as ISO/IEC 27001, and frameworks, such as the NIST Cybersecurity Framework, have provided guidance to organizations on how to implement effective controls to mitigate risks (Accerboni & Sartor, 2019; Shen, 2014).

However, the implementation of existing controls is not always effective in all scenarios. Gartner (2020) reported that more than 60% of organizations fail to manage application risk well, even though they implement sophisticated security technologies. This shows a gap between the expected risk control and the reality of its implementation in the field. One of the reasons for this failure is an approach that focuses too much on responding to incidents rather than creating system resilience that is able to face attacks and threats that continue to evolve.

Resilience in the context of application system security refers to the ability of a system to continue functioning or recover quickly despite an incident or disruption. This concept emphasizes the importance of planning, proactive risk assessment, and strengthening application systems so that they can not only

survive attacks but also recover quickly to minimize business impact. According to research by Accenture (2021), organizations that focus on improving their cyber resilience manage to reduce the impact of cyberattacks up to 30% faster than organizations that do not have an adequate resilience strategy.

Therefore, a review of the existing literature on application system risk, security controls, and risk management is essential. Using a systematic review approach that follows the PRISMA guidelines, this study aims to identify trends, effectiveness of security control strategies, and best practices in building application system resilience across sectors. This study will present empirical evidence from various studies to provide strong guidance for organizations in managing risk and building resilience in the future.

Methods

Procedure

The Systematic Literature Review (SLR), a literature review method, identifies, evaluates, and interprets all findings on a research topic to address previously established research questions (Budgen, Kitchenham, Charters, Turner, Brereton, & Linkman, 2007).

The literature search was limited to articles published in 2020-2024, on October 5, 2024. The article search was conducted using the Publish or Perish (PoP) software program using the search words "Application System Risks AND Security Controls AND Risk Management" in the title and keywords in the research databases in Google Scholar and Scopus.

Analysis

The method used is the Preferred Reporting Item for Systematic Reviews and Meta-Analytic (PRISMA) method. All articles that pass the selection are then reviewed and summarized based on the objectives, author's name, year of publication, number of respondents, instruments used, research results, and suggestions for further research.

Inclusion criteria include 1) research on risk identification, implementation of security controls, and transformation towards resilience in application systems, 2) published in the form of research articles. Exclusion criteria include 1) literature review articles or meta-analyses. The search process begins by reviewing the titles and abstracts of all search results and comparing them with the established criteria.

The research database search resulted in all keyword search results obtaining 400 research articles, from Google Scholar as many as 200 and Scopus as many as 200 articles. After scanning the title, there were the same articles in different databases. The results after reducing duplicates were 398 articles. A total of 212 findings were excluded because they were books (21), book chapters (9), conference papers (71) and literature reviews (111). In addition, there were 159 articles that did not meet the criteria, namely in the form of business, finance, and economics (15), agriculture, environmental science, and sustainability (21), artificial intelligence (AI), machine learning, and technology (20), health, medicine, and public safety (21), engineering and industrial systems (24), education and research (13), environmental management and policy (10), public policy and governance (8), energy systems and sustainability (11), food and agriculture technology (8), and miscellaneous/other (12). There are 23 articles included in the literature review. Literature search is described in more detail in Figure 1.

Research Mapping

We conducted research mapping on the topic of application system security control and risk management to strengthen the foundation of our study. The mapping process was carried out to determine the mapping of keywords from the research topic. The articles were analyzed using VOSviewer, a software that describes, organizes, and visualizes bibliometric data. This application supports mapping through clustering models and layout techniques, with displays such as overlays and density visualizations. VOSviewer helps summarize big data, shows intellectual structures, and identifies research trends (Van Eck & Waltman, 2010). Furthermore, articles were classified by subtopic to determine popular research fields and methodologies.

The results are then visualized using VOSviewer, as shown in Figure 2. Figure 2 visualizes the results of the article keyword mapping. It can be seen in Figure 2 that the mapping results are divided into three clusters, represented by three different colors. In VOSviewer, a cluster refers to a group of items visible on the map, where each item represents a term. Color is used by VOSviewer to indicate the cluster in which an item is located (Perianes-Rodriguez, Waltman, & Van Eck, 2016).

Figure 2 depicts a complex conceptual map of cybersecurity issues, especially in the context of application development. This visual analysis shows that current research in this field focuses heavily on the interaction between technology, applications, and security risks. The concept of "application" is at the center of the network, indicating that applications are a focal point in various studies. Technologies such

as blockchain and artificial intelligence (AI) are closely connected to the concept of application, indicating the integration of these technologies in secure application development. Meanwhile, security risks such as threats, vulnerabilities, and risk assessments are of primary concern, reflecting the growing concern about potential cyberattacks. The context of "smart cities" also appears, indicating that cybersecurity issues are not only relevant at the individual or organizational scale but also at the urban infrastructure scale. Overall, this conceptual map highlights the complexity of cybersecurity issues and shows a shifting research trend towards developing more comprehensive and adaptive security solutions to technological developments.

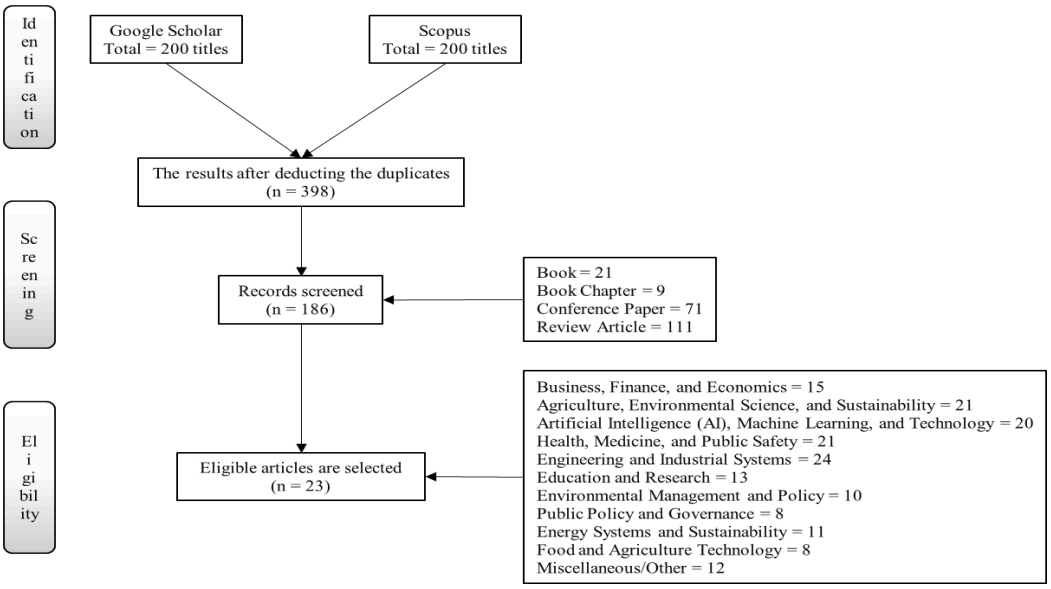

Figure 1
Literature Review Search Method

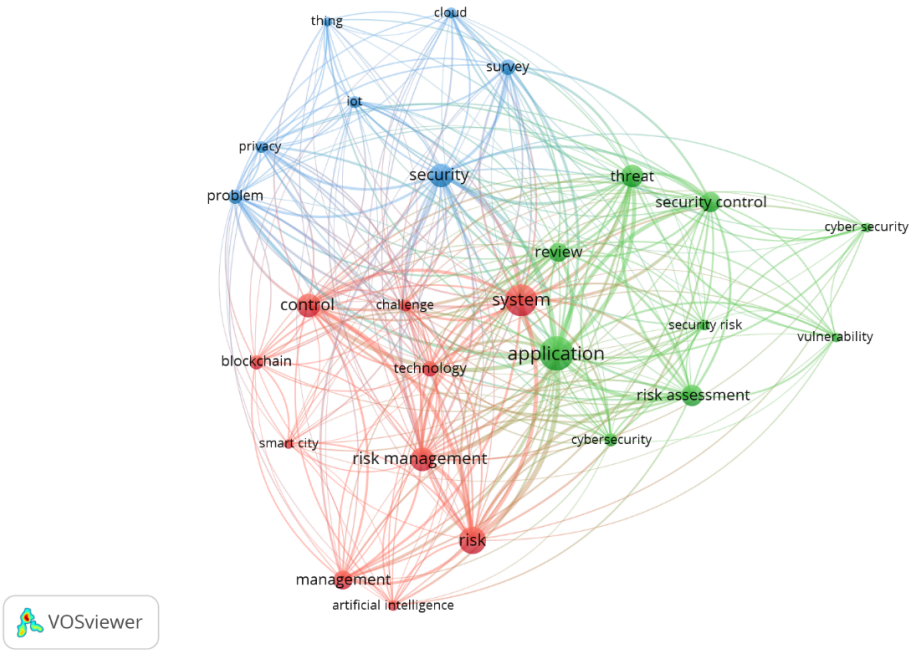

Figure 2
Research Mapping

Results and Discussions

The results and discussion section contains research findings, data analysis based on a literature review relevant to the research objectives, and a discussion of topics related to the results.

Table 1. Literature Review on Cybersecurity and Risk Management Topics

No.	Topics	Author
1	Cybersecurity Evaluation Frameworks	H. Zhang, Pan, Lu, Wang, & Liu (2021)
2	Industrial Cybersecurity Trends and Countermeasures	Alladi, Chamola, & Zeadally (2020)
3	Policy Compliance and Security Management	Hina & Dominic (2020)
4	Smart Grid Cybersecurity Challenges	Dong, Cao, Flynn, & Fan (2022)
5	Risk Management Frameworks	Lee (2021)
6	Risk Assessment in Specific Domains	Chen, Zheng, Li, & Huang (2021); Li, Wang, Wang, Shao, & He (2020)
7	Blockchain and Resilient Security Controls	Madine, Battah, Yaqoob, Salah, Jayaraman, Al-Hammadi, Pesic, & Ellahham (2020); Singh, Sharma, Yoon, Shojafar, Cho, & Ra (2020); Xu, Zhang, Cliff, & Ma (2022)
8	Cloud Security and Risk Management	Gopalakrishnan & Alli (2021); Mughal (2021); Paulraj, Neelakandan, Prakash, & Baburaj (2023)
9	Autonomous Systems Security	D. Zhang, Shen, Zhou, Dong, & Yu (2020)
10	Blockchain Applications in IoT and Smart Cities	Asif, Aziz, Bin Ahmad, Khalid, Waris, & Gilani (2022); HS (2022); Zhu, Huang, Hu, Al-Dhelaan, & Al-Dhelaan (2021)
11	Construction IoT Risk Management	Liang & Liu (2022)
12	Renewable Energy Cybersecurity	de Peralta, Watson, Bays, Boles, & Powers (2021)
13	Smart Cities Security Challenges	Gunduz & Das (2020); Kitchin & Dodge (2020); Rios, Rego, Iturbe, Higuero, & Larrucea (2020)
14	Smart Grid Optimization and Analytics	Panda & Das (2021)

Source: Data Processing Result, 2024

Cybersecurity Evaluation Frameworks

Based on the literature review, there is one article that examines the evaluation approach and cybersecurity framework for vehicle electronic control systems. H. Zhang *et al.* (2021) successfully developed a cybersecurity evaluation framework for electronic control units (ECUs) in vehicles. This framework is designed to identify, analyze, and evaluate cybersecurity vulnerabilities in modern vehicle ECU systems. Their approach includes a quantitative method to assess security risks based on technical characteristics and exploitability. The results show that this framework can provide effective guidance for improving cybersecurity in vehicles, assisting manufacturers in developing more secure ECU systems.

Industrial Cybersecurity Trends and Countermeasures

Alladi *et al.* (2020) found that industrial control systems (ICS) face increasing threats from cyberattacks, including ransomware, malware-based attacks, and exploiting communication vulnerabilities. The authors highlight the trend of increasingly sophisticated cyberattacks against ICS and targeting critical infrastructure. The article also summarizes various mitigation measures and security approaches, such as the use of encryption, multi-factor authentication, network segmentation, and intrusion detection systems. In conclusion, protecting ICS requires a proactive and adaptive security strategy to address the evolving threat landscape.

Policy Compliance and Security Management

The article by Hina & Dominic (2020) concluded that compliance with information security policies in higher education institutions is influenced by a variety of factors, including awareness, organizational culture, and management support. The study highlights the importance of a holistic approach to designing and implementing information security policies, involving ongoing training and effective communication. The authors also emphasize that increasing staff and student understanding of the importance of information security is key to minimizing the risk of breaches and increasing compliance with policies.

Smart Grid Cybersecurity Challenges

The article by Dong *et al.* (2022) concludes that cybersecurity is a crucial element in smart local energy systems. The authors identify various requirements, challenges, and standards related to cybersecurity in this sector. The main challenges include increasing vulnerabilities due to system complexity, device interoperability, and resource constraints. The article also discusses the need for a robust security framework, which includes threat detection, risk management, and data protection. The authors emphasize the importance of adopting international standards and developing technology-based approaches and policies to effectively address cyber threats in smart energy systems.

Risk Management Frameworks

Lee (2021) concludes that cybersecurity risk management requires a structured framework and a strategic approach to investment allocation. The author introduces a risk management framework that helps organizations identify cyber threats, evaluate their impact, and prioritize mitigation measures. The article also highlights the importance of analyzing the cost of investment to ensure that cybersecurity spending is commensurate with its benefits, such as risk reduction and protection of organizational assets. Lee emphasizes that investment decisions should be based on a balance between the cost of protection and the value of the risk that can be minimized, thereby supporting long-term business sustainability.

Risk Assessment in Specific Domains

The article by Li *et al.* (2020) concluded that the combination of Fuzzy Analytical Hierarchy Process (Fuzzy AHP) and Bayesian Network (BN) methods is effective in assessing the risk of gas explosions in coal mines. This study developed a model that integrates data uncertainty with causal structure to identify key risk factors, such as poor ventilation, high gas concentration, and failure of the monitoring system. This model helps prioritize mitigation measures based on the probability and impact of the risk. The authors emphasize that this approach can be used as a powerful decision-making tool to improve safety in coal mines, minimize incidents, and protect workers and assets.

The article by Chen *et al.* (2021) concluded that the Random Forest algorithm can be used effectively to assess security risks and provide early warnings in large group events. This study developed a data-driven model that identifies key risk factors, such as crowd density, location characteristics, and event management. The model showed high accuracy in predicting potential risks and providing early warnings that allow for preventive actions. The authors emphasized that this approach can help large event organizers improve safety by supporting data-driven decisions and strengthening proactive risk management.

Blockchain and Resilient Security Controls

The article by Singh *et al.* (2020) concludes that the convergence of blockchain technology and artificial intelligence (AI) in the Internet of Things (IoT) network can provide a sustainable solution for smart city management. The authors show that this integration can improve data security, operational efficiency, and real-time decision-making in various smart city applications, such as transportation, energy, and waste management. Blockchain provides transparency and trust through secure data storage, while AI enables complex data analysis to support automation and prediction. The article highlights that this approach not only improves the sustainability of smart cities but also addresses key challenges such as scalability, privacy, and resource management effectively.

The article by Xu *et al.* (2022) concludes that they developed an efficient blockchain-based scheme to preserve data privacy, using attribute encryption and homomorphic encryption. This approach enables secure and protected data exchange in decentralized systems without compromising user privacy. By using attribute encryption, only authorized parties can access specific data, while homomorphic encryption allows processing of encrypted data without the need to decrypt it. The authors emphasize that this scheme not only enhances data security in blockchain-based applications but also supports stronger privacy protection, which is critical in applications such as finance and healthcare.

The article by Madine *et al.* (2020) concludes that blockchain technology can provide patients with greater control over their medical records in a secure, transparent, and decentralized manner. The authors propose a blockchain-based system that allows patients to manage access to their medical records, ensuring that the data remains protected from manipulation and information leakage. By leveraging blockchain's advantages in terms of security, transparency, and auditability, the system enables the exchange of medical information between healthcare providers more efficiently and securely. In conclusion, the application of blockchain in medical records management can improve patient privacy, accelerate access to medical information, and strengthen individual control over their health data.

Cloud Security and Risk Management

The article by Paulraj *et al.* (2023) concludes that anonymous identity-based access control and key agreement policies can improve security and privacy in cloud computing. The author proposes an approach that combines strict access control with a key agreement mechanism to ensure secure communication between users and cloud service providers without revealing the user's true identity. By using anonymous identities, this system protects user privacy and reduces the risk of attacks on personal data. In conclusion, this approach has the potential to improve privacy protection in cloud computing services, ensuring secure and efficient access to cloud resources without compromising the confidentiality of user identities.

The article by Gopalakrishnan & Alli (2021) concludes that trust-based approaches and risk management are essential in cloud service selection for IT systems. The authors propose a model that integrates trust level evaluation and risk analysis to help organizations select the most reliable and secure cloud service providers. By considering factors such as performance, compliance with security standards, and the level of risk associated with the service provider, the model enables better decision-making in selecting cloud services. In conclusion, this approach provides a more holistic and measurable framework for selecting cloud service providers that meet organizational needs effectively and securely.

The article by Mughal (2021) concludes that an effective cybersecurity architecture is essential to protect networks in a cloud computing virtualization environment. The author highlights the various challenges faced in maintaining data and infrastructure security in the cloud, such as DDoS attacks, leaks, and internal threats. The article proposes the use of a layered security approach that includes access control, data encryption, and continuous monitoring to identify threats in real-time. In conclusion, implementing a robust security architecture in cloud computing can ensure data integrity, confidentiality, and availability, as well as increase resilience to cyberattacks in a virtualized environment.

Autonomous Systems Security

The article by D. Zhang *et al.* (2020) concludes that secure distributed platoon control for connected vehicles can be successfully implemented despite Denial-of-Service (DoS) attacks. The authors develop a control theory and approach that allows vehicles in a platoon to continue operating efficiently and safely despite being affected by cyberattacks aimed at disrupting inter-vehicle communications. By using model-based control techniques that integrate redundancy and mitigation strategies, the system can maintain platoon performance and reduce the risk of system failure. In conclusion, this article shows that with proper control, connected vehicles can overcome cyber threats such as DoS attacks while maintaining operational safety and efficiency.

Blockchain Applications in IoT and Smart Cities

The article by HS (2022) concludes that reputation management in vehicle networks can be significantly improved using blockchain technology. The authors propose the implementation of a blockchain-based system to verify and monitor the reputation of vehicles and entities involved in the vehicle network. By leveraging the characteristics of blockchain, such as transparency and the impossibility of changing recorded data, this system can prevent fraud, ensure the reliability of communication between vehicles, and improve overall security. In conclusion, the use of blockchain in reputation management can strengthen trust and operational efficiency in interconnected vehicle networks.

The article by Zhu *et al.* (2021) concluded that a blockchain-based access management system can be effectively applied to edge computing, providing better security and access control solutions. The authors developed a system that combines blockchain to manage and verify access to resources in edge computing, which has the characteristics of decentralization and resource constraints. By using blockchain, the system ensures that only authorized entities can access data or services while providing data transparency and integrity. In conclusion, this approach improves the security and efficiency of

access management in edge computing environments and protects data and applications from potential threats and misuse.

The article by Asif *et al.* (2022) concludes that blockchain-based authentication and trust management mechanisms can significantly improve security and trust in smart city environments. The authors propose a system that leverages blockchain to ensure secure authentication between entities involved in a smart city ecosystem, such as IoT devices, users, and service providers. By using smart contracts and a decentralized ledger, the system can increase transparency, prevent data manipulation, and ensure that only authorized entities can access critical services and information. In conclusion, the application of blockchain in trust management and authentication can strengthen the integrity and security of smart cities, improve operational efficiency, and reduce the risk of potential cyberattacks.

Construction IoT Risk Management

The article by Liang & Liu (2022) concluded that the use of Building Information Modeling (BIM) and the Internet of Things (IoT) can effectively improve early warning and control of construction safety risks in underground engineering projects. The authors developed a system that integrates BIM for project modeling and visualization with IoT for real-time condition monitoring. This system can detect potential safety risks, such as ground movement, moisture, or structural failure, and provide early warning for preventive actions. In conclusion, the integration of BIM and IoT helps improve safety in underground construction projects by enabling rapid response to emerging risks and minimizing the possibility of accidents.

Renewable Energy Cybersecurity

The article by de Peralta *et al.* (2021) concludes that to ensure cyber resilience in marine renewable energy systems, it is essential to adopt best practices in cybersecurity and risk management. The authors identify various steps that should be taken to protect these systems from cyber threats, such as continuous monitoring, strict access management, and the implementation of encryption to protect data. They also emphasize the importance of collaboration between industry stakeholders, as well as training and awareness for the workforce regarding cyber threats. In conclusion, the implementation of best practices and effective risk management strategies can improve the resilience of marine renewable energy systems to increasingly complex cyber threats.

Smart Cities Security Challenges

The article by Kitchin & Dodge (2020) concludes that smart cities face a range of vulnerabilities related to cyber threats and risks arising from reliance on connected technologies. The authors identify weaknesses in smart city infrastructure, including issues related to data collection and management, as well as potential security gaps in systems connecting IoT devices, transportation, energy, and public services. They propose a mitigation approach involving the implementation of stricter policies, encryption technologies, and an integrated security framework. In conclusion, to mitigate the risks associated with their vulnerabilities, it is important for smart cities to develop a comprehensive security strategy, engage stakeholders, and increase awareness and training on cyber threats and protection.

The article by Rios *et al.* (2020) concludes that continuous quantitative risk management in smart grids can be effectively implemented using attack-defense trees. The authors propose an attack and defense tree-based approach to analyze potential threats to smart grid infrastructure as well as to plan optimal mitigation measures. By modeling possible attacks and corresponding defense responses, the system enables more accurate risk assessments and helps in better decision-making in managing threats to grid stability and reliability. In conclusion, the use of attack-defense trees in smart grids can improve resilience to attacks and provide a stronger basis for more scalable and responsive risk management strategies.

The article by Gunduz & Das (2020) concludes that smart grids are vulnerable to various cyber threats that can affect the reliability and integrity of the energy system. The authors identify various types of possible attacks, such as DDoS attacks, data manipulation, and intrusions into the energy distribution control system. To address these threats, they propose solutions that include the implementation of encryption technologies, stronger authentication, and the use of more sophisticated intrusion detection systems. In conclusion, to improve cybersecurity in smart grids, a comprehensive approach is needed that involves strengthening data protection, continuous monitoring, and more adaptive mitigation strategies against potential evolving attacks.

Smart Grid Optimization and Analytics

The article by Panda & Das (2021) concludes that the implementation of advanced smart grid architecture models is essential for control, optimization, and data analytics in future power grids, especially with greater integration of renewable energy. The authors propose an architecture model that leverages the latest technologies to improve the operational efficiency of the power grid, optimize energy distribution, and analyze data in real-time to respond to dynamic changes in demand and supply. The model also takes into account the challenges associated with the integration of volatile renewable energy resources, such as solar and wind. In conclusion, an integrated smart grid model with data-driven control and optimization will enable a smarter, more efficient, and greener power system to face future challenges.

Conclusions

These articles discuss the topic of application system security controls and risk management from 2020–2024. Using a meta-analysis approach with the PRISMA methodology, this study collected data from two major databases, namely Google Scholar and Scopus, which resulted in 23 relevant articles. From the 23 articles, 14 subtopics related to application system security controls and risk management were identified. The conclusion from the summary of the articles above shows that to face the challenges of security and efficiency in increasingly complex smart grid systems, especially with the integration of renewable energy, various approaches and technologies need to be applied. The use of blockchain, IoT, and Building Information Modeling (BIM) can strengthen security and risk management, while intelligent smart grid architecture allows for more efficient control and optimization of energy distribution. On the other hand, to maintain resilience to cyber threats, it is important to develop a system that combines encryption, intrusion detection, and data-driven risk management. With this holistic approach, smart grids can be more secure, efficient, and able to support the transition to a more sustainable energy system.

References

Accenture. (2021). Building Cyber Resilience in a Digital-First World. Retrieved from www.accenture.com

Accerboni, F., & Sartor, M. (2019). ISO/IEC 27001. In *Quality Management: Tools, Methods, and Standards* (pp. 245-264): *Emerald Publishing Limited*.

Alladi, T., Chamola, V., & Zeadally, S. (2020). Industrial Control Systems: Cyberattack Trends and Countermeasures. *Computer Communications, 155*, 1-8.

Asif, M., Aziz, Z., Bin Ahmad, M., Khalid, A., Waris, H. A., & Gilani, A. (2022). Blockchain-Based Authentication and Trust Management Mechanism for Smart Cities. *Sensors, 22*(7), 2604.

Budgen, D., Kitchenham, B., Charters, S., Turner, M., Brereton, P., & Linkman, S. (2007). *Preliminary Results of a Study of the Completeness and Clarity of Structured Abstracts*. Paper presented at the *11th International Conference on Evaluation and Assessment in Software Engineering (EASE)*.

Chen, Y., Zheng, W., Li, W., & Huang, Y. (2021). Large Group Activity Security Risk Assessment and Risk Early Warning Based on Random Forest Algorithm. *Pattern Recognition Letters, 144*, 1-5.

de Peralta, F. A., Watson, M. D., Bays, R. M., Boles, J. R., & Powers, F. E. (2021). Cybersecurity Resiliency of Marine Renewable Energy Systems Part 2: Cybersecurity Best Practices and Risk Management. *Marine Technology Society Journal, 55*(2), 104-116.

Deloitte. (2021). Cybersecurity in the Age of Digital Transformation: Strengthening Security and Resilience. Retrieved from www2.deloitte.com

Dong, S., Cao, J., Flynn, D., & Fan, Z. (2022). Cybersecurity in Smart Local Energy Systems: Requirements, Challenges, and Standards. *Energy Informatics, 5*(1), 9.

Gartner. (2020). Risk Management Failure in Application Systems: Causes and Solutions. Retrieved from www.gartner.com

Gopalakrishnan, S., & Alli, P. (2021). Trust Based Approach and Risk Management for IT Systems in Cloud Service Selection. *Wireless Personal Communications, 117*, 3109-3127.

Gunduz, M. Z., & Das, R. (2020). Cyber-Security on Smart Grid: Threats and Potential Solutions. *Computer networks, 169*, 107094.

Hina, S., & Dominic, P. D. D. (2020). Information Security Policies' Compliance: A Perspective for Higher Education Institutions. *Journal of Computer Information Systems*.

HS, J. (2022). Reputation Management in Vehicular Network Using Blockchain. *Peer-to-Peer Networking and Applications, 15*(2), 901-920.

IBM Security. (2021). Cost of A Data Breach Report 2021. *Risk Quantification, 73*.

Kaspersky. (2020). The Global State of Cybersecurity: Threats and Solutions. Retrieved from www.kaspersky.com

Kitchin, R., & Dodge, M. (2020). The (in) Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. In *Smart Cities and Innovative Urban Technologies* (pp. 47-65): Routledge.

Lee, I. (2021). Cybersecurity: Risk Management Framework and Investment Cost Analysis. *Business Horizons, 64*(5), 659-671.

Li, M., Wang, H., Wang, D., Shao, Z., & He, S. (2020). Risk Assessment of Gas Explosion in Coal Mines Based on Fuzzy AHP and Bayesian Network. *Process Safety and Environmental Protection, 135*, 207-218.

Liang, Y., & Liu, Q. (2022). Early Warning and Real-Time Control of Construction Safety Risk of Underground Engineering Based on Building Information Modeling and Internet of Things. *Neural Computing and Applications*, 1-10.

Madine, M. M., Battah, A. A., Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y., . . . Ellahham, S. (2020). Blockchain for Giving Patients Control Over Their Medical Records. *IEEE Access, 8*, 193102-193115.

Mughal, A. A. (2021). Cybersecurity Architecture for the Cloud: Protecting Network in a Virtual Environment. *International Journal of Intelligent Automation and Computing, 4*(1), 35-48.

Panda, D. K., & Das, S. (2021). Smart Grid Architecture Model for Control, Optimization and Data Analytics of Future Power Networks with More Renewable Energy. *Journal of Cleaner Production, 301*, 126877.

Paulraj, D., Neelakandan, S., Prakash, M., & Baburaj, E. (2023). Admission Control Policy and Key Agreement Based on Anonymous Identity in Cloud Computing. *Journal of Cloud Computing, 12*(1), 71.

Perianes-Rodriguez, A., Waltman, L., & Van Eck, N. J. (2016). Constructing Bibliometric Networks: A Comparison Between Full and Fractional Counting. *Journal of informetrics, 10*(4), 1178-1195.

Rios, E., Rego, A., Iturbe, E., Higuero, M., & Larrucea, X. (2020). Continuous Quantitative Risk Management in Smart Grids Using Attack Defense Trees. *Sensors, 20*(16), 4404.

Shen, L. (2014). The NIST Cybersecurity Framework: Overview and Potential Impacts. *Scitech Lawyer, 10*(4), 16.

Singh, S., Sharma, P. K., Yoon, B., Shojafar, M., Cho, G. H., & Ra, I.-H. (2020). Convergence of Blockchain and Artificial Intelligence in IoT Network for the Sustainable Smart City. *Sustainable cities and society, 63*, 102364.

Van Eck, N., & Waltman, L. (2010). Software Survey: VOSviewer, A Computer Program for Bibliometric Mapping. *scientometrics, 84*(2), 523-538.

Xu, G., Zhang, J., Cliff, U. G. O., & Ma, C. (2022). An Efficient Blockchain‐Based Privacy‐Preserving Scheme with Attribute and Homomorphic Encryption. *International Journal of Intelligent Systems, 37*(12), 10715-10750.

Zhang, D., Shen, Y.-P., Zhou, S.-Q., Dong, X.-W., & Yu, L. (2020). Distributed Secure Platoon Control of Connected Vehicles Subject to DoS Attack: Theory and Application. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51*(11), 7269-7278.

Zhang, H., Pan, Y., Lu, Z., Wang, J., & Liu, Z. (2021). A Cyber Security Evaluation Framework for in-Vehicle Electrical Control Units. *IEEE Access, 9*, 149690-149706.

Zhu, Y., Huang, C., Hu, Z., Al-Dhelaan, A., & Al-Dhelaan, M. (2021). Blockchain-Enabled Access Management System for Edge Computing. *Electronics, 10*(9), 1000.