J. Electrical Systems 20-10s (2024): 7989-8001

[1] **Abdulmalik Ahmad Lawan**
[2] **Abdullahi Aliyu Danlami**
[3] **Samuel-Ajakaiye Kehinde**
[4] **Bashir Aliyu**
[5] **Aliyu Hassan Abdullahi II**

Blockchain-Empowered Cybersecurity Solutions Across Diverse Application Domains: A Survey

Journal of Electrical Systems

Abstract: - Blockchain technology has emerged as a transformative force in cybersecurity, offering decentralized, transparent, and immutable mechanisms for securing critical data and transactions across diverse application domains. Through a systematic literature review, the present study explored the utilization of blockchain technology in enhancing cybersecurity solutions across various sectors, including defense, healthcare, industries, smart cities, energy systems, and communication networks. Descriptive analysis and thematic synthesis of the relevant literature identified the key applications of blockchain in cybersecurity, highlighting emerging trends, opportunities, and challenges in blockchain integration into cybersecurity frameworks. Insights and recommendations for future research and practical implementation are provided, aiming to contribute to a deeper understanding of the potential of blockchain technology in enhancing both the traditional and future cybersecurity ecosystems.

Keywords: Blockchain, Blockchain integration, Cybersecurity, Data security, Healthcare cybersecurity, Energy systems security, Industrial cybersecurity, Smart cities security, Systematic literature review.

I. INTRODUCTION

With increasing reliance on interconnected systems and the proliferation of sophisticated cyber threats that necessitate the need for robust, reliable, and innovative solutions, cybersecurity has become a key concern across various application domains, including defense [1], [2], [3], [4], healthcare [5], [6], [7], industrial systems [8], [9], [10], and smart cities [11], [12], [13]. Blockchain technology, originally conceptualized as the underlying infrastructure for cryptocurrencies, is recently viewed in academia and industry as a transformative tool to address pressing cybersecurity challenges due to its decentralized, transparent, and immutable nature [14], [15], [16], [17]. In addition, blockchain involves mechanisms such as consensus algorithms, cryptographic hashing, and smart contracts that provide unique advantages for securing critical data and transactions across diverse application domains [18], [19], [20], [21], [22].

Recent studies have explored the integration of blockchain technology into various cybersecurity frameworks, highlighting its revolutionary potential in protecting sensitive, particularly, demonstrating blockchain's efficacy in securing communication networks, protecting critical infrastructure, and ensuring the integrity of sensitive data [1], [2], [3], [4], [8], [9], [10], [11], [12], [13], [14], [15], [16], [23]. However, while existing literature provided valuable insights into the applications of blockchain in specific domains, there is insufficient analysis and synthesizes of recent findings across multiple application domains [15], [16]. In essence, existing studies often focus on theoretical frameworks or isolated case studies, lacking a holistic perspective on the practical challenges, opportunities, and future directions of blockchain-empowered cybersecurity solutions.

Based on a systematic literature review, the present manuscript aims to address this research gap by providing a systematic review of the utilization of blockchain technology in enhancing cybersecurity solutions across various sectors, including defense, healthcare, industrial systems, smart cities, energy systems, and communication networks. Through a descriptive analysis and thematic synthesis of the relevant literature, this study identifies key applications, emerging trends, and challenges associated with blockchain integration into cybersecurity frameworks. The insights and recommendations provided in this manuscript are intended to contribute to a deeper understanding of the potential of blockchain technology in fortifying traditional and future cybersecurity ecosystems. By offering a comprehensive survey of blockchain-empowered cybersecurity solutions across diverse

[1] Department of Computer Science, Aliko Dangote University of Science and Technology, Wudil, Nigeria. aalawan@kustwudil.edu.ng
[2] Department of Manufacturing Services, National Agency for Science and Engineering Infrastructure (NASENI), Abuja, Nigeria. danboko@naseni.gov.ng
[3] Department of Manufacturing Services, National Agency for Science and Engineering Infrastructure (NASENI), Abuja, Nigeria. samuel.kehinde@naseni.gov.ng and African University of Science and Technology (AUST). ksamuel@aust.edu.ng
[4] National Agency for Science and Engineering Infrastructure (NASENI), Abuja, Nigeria. bashir.aliyu@naseni.gov.ng
[5] Department of Computer Science, Federal Polytechnic Nasarawa, Nasarawa, Nigeria. hasabujabir@gmail.com

application domains, this study seeks to inform both researchers and practitioners on the state of the art and guide future research and practical implementations in this critical area.

II. METHODOLOGY

2.1 Search Strategy

The methodical investigation of the present study was conducted in September 2023 to systematically search for relevant studies aimed at approaching the research question. The data collection, reading, and systematic literature were logically planned and conducted by the authors. A holistic systematic search was carried out on the relevant databases to the topic namely: Web of Science, IEEEXplore, Scopus, and ACM Digital Library. The search terms utilized were "Cybersecurity" and "Blockchain" and the search filters were set to extract records of the articles published in English from 2013 upwards.

2.2 Selection Criteria

PRISMA [24] systematic review procedure was utilized to select the most relevant articles to be included in the study. The criterion for inclusion in the present study covered any published full-text journal article, book chapter, or conference paper, from the indicated databases, on the application of blockchain in various domains that employ cybersecurity solutions. At the beginning of data screening, duplicate articles retrieved from multiple databases were eliminated using the duplicate-removal function of Microsoft Excel version 2019. Then, the authors advanced the inclusion criteria by scrutinizing worthy papers to be synthesized in the systematic literature review. The decisions for inclusion/exclusion of the unique records were recorded in a separate column within the combined Excel sheet imported from the multiple databases. Table 1 provides a summary of the inclusion/exclusion criteria of the present study. Thus, for documents whose titles and corresponding abstracts aligned with the preset inclusion criteria, full-text articles of the studies were retrieved for the subsequent screening stage. In the next PRISMA screening stage, all the downloaded papers were reviewed to ascertain their relevance with the search query and the preset research question.

Table 1: Inclusion/exclusion criteria

Inclusion Criteria	Exclusion Criteria
Records from specified databases (Web of Science, IEEEXplore, Scopus, ACM Digital Library)	Duplicate records
Records of articles published in English	Articles published in other languages
Records of articles published from 2013 to date	Articles not meeting the preset inclusion period
Published full-text journal articles, book chapters, or conference papers	Articles not relevant to the study's aim
Records of studies on cybersecurity solutions using blockchain technology	Articles not related to cybersecurity or blockchain
Articles whose titles and abstracts align with preset inclusion criteria	Articles with ambiguous contents
Full-text articles of studies whose titles and abstracts align with preset inclusion criteria	Articles whose full text is not available

Specifically, eight hundred and ninety-nine records were carefully assessed for eligibility. Three hundred and Thirty-one unique papers remained after data cleaning that involved removing duplicates and records with so many missing values. Fifty-two editorial materials (n = 52), nine Non-English records (n = 9), thirty-five unavailable (n = 35), and short review (n = 43) records were further eliminated. Ninety-five unrelated studies were removed despite having some of the search keywords (n = 95), and relevant studies with no specific focus on any application domain (n = 24) were equally exempted. The final exclusion activity involved eleven (n = 11), four (n = 4), and (n = 12) were eliminated due to lot of ambiguities, deviation from the research aim, and focus on theoretical ideas, respectively. Consequently, forty-six (n = 46) full-text articles were retrieved, read, and qualitatively assessed. The PRISMA flow diagram (Figure 1) summarized the abovementioned systematic literature review process.

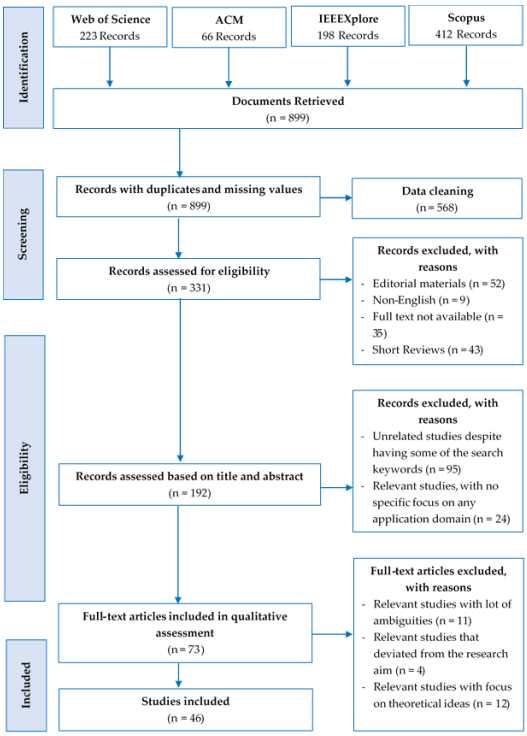

Figure 1. PRISMA flow diagram of the search results

2.3 Quality Assessment

The authors carefully adhered to the planned, systematic literature review process to maintain the quality of the study. Notably, the authors ensured careful adherence to the adopted research framework at every phase of the systematic literature review. Furthermore, all the downloaded articles were uploaded to an online Mendeley repository to keep track of the appropriate citations to the literature and aid in information sharing, data extraction, and classification stages. Nevertheless, unbiased and constructive assessments of the systematic approach used in this study were sought from external professionals on educational intervention for learners with disability and with expertise in systematic literature reviews.

2.4 Data Extraction

In the final stage of the study's PRISMA, the data extraction stage, 46 articles were appraised critically and utilized in structuring the thematic discussion of the literature based on year of publication, source title and publisher, dimensions of cybersecurity and blockchain considered as well as the application area.

III. RESULTS

3.1 Descriptive Analysis of the Literature

Based on the exported data, the trend of studies on Systematic Literature Review on the Application of Cybersecurity and Blockchain in Secured-IOT showed the most researched technologies and study design, most cited references, sources, the country of research, and citation and publication frequencies over the years.

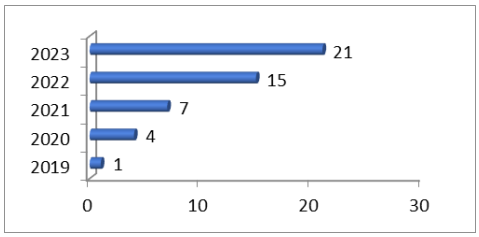

Figure 2. Number of publications across years

With the rising prevalence of cyber security coupled with the increasing popularity of Block chain practice, there will be growing demand for sustainable strategies for cyber security using the IOT technologies. Notably, as shown in Figure 2, from 2023 to 2019, not many studies cared about the subject area. However, with the recently increased patronage of various technologies in supporting different educational strategies, there is the possibility of more future studies on Systematic Literature Review on the Application of Cybersecurity and Blockchain in Secured-IOT. Obviously, in the future, it can be said that the trend will go on.

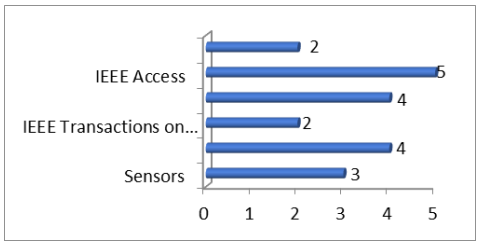

Figure 3. Most frequent sources

From Figure 3, most of the articles contributing to the area were published in the *IEEE Access* (n = 5), followed by the IEEE internet of things journal and *IEEE Transactions on Industrial informatics* (n = 4, each). Others were sensors (n = 3), Electronics (Switzerland) and IEEE Transactions on Industrial Informatics (n = 2 each), while each of the remaining journals featured in the inclusion list published one article. In addition, IEEE published most of the study area articles (n = 12), as shown in Figure 4.

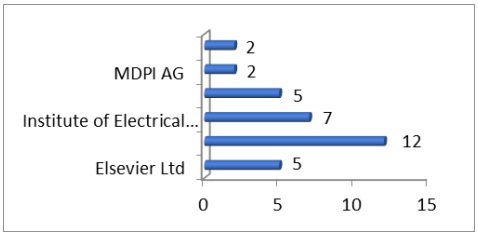

Figure 4. Number of articles based on publishers

Based on the citation data analysed in the present study, the most cited references are Smith et al. [34] (n = 115), Rosenbloom et al. [12] (n = 35), and Knight et al. [35] (n = 32). These references contributed the most citations in the past, as shown in Figure 5, as they were published in Cybersecurity and Blockchain, respectively.

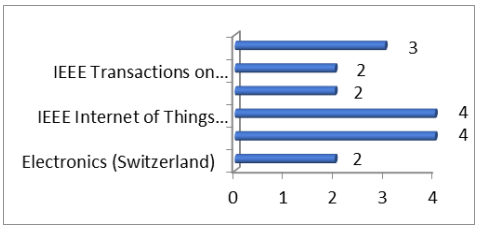

Figure 5. Most frequent citations based on sources

The citation distribution across years, as shown in Figure 6, indicated the relevance of the past publications on the research topic by attaining high citation counts.

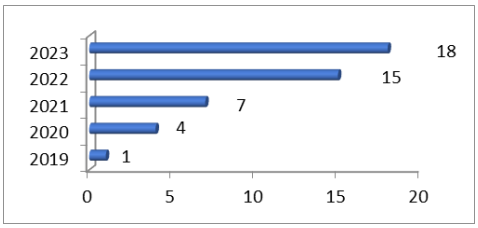

Figure 6. Number of citations across years

From Figure 7, the included studies were predominantly conducted in the USA (n = 13) and a few from Ecuador (n = 3), France (n = 2), and Italy (n = 2). Thus, out of the 36 articles included in the study, the countries mentioned above contributed more to the research area, followed by other countries depicted in the figure that contributed single articles each and one multinational study conducted in Russia and Brazil [20].

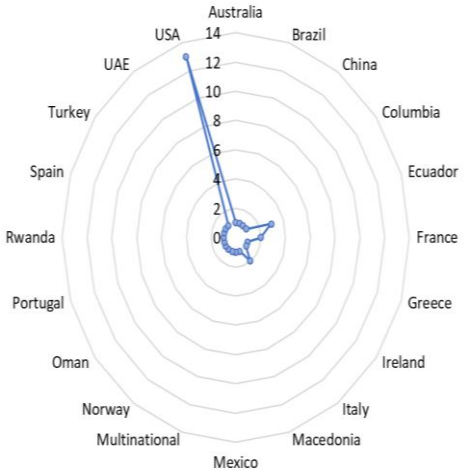

Figure 7. Number of articles based on country of research.

Descriptive findings that are of the essence to ASD-inclusive education and research are the most popular technologies utilized in the study area, as well as the frequently used research designs. As shown in Figure 8, most studies utilized a mixed study design (n = 17) to understand the efficacy of emerging computer technologies in supporting ASD-inclusive education. Other studies were case studies (n = 3), experimental (n = 6), and implementation (n = 7) studies that developed and evaluated various technologies for ASD-inclusive education.

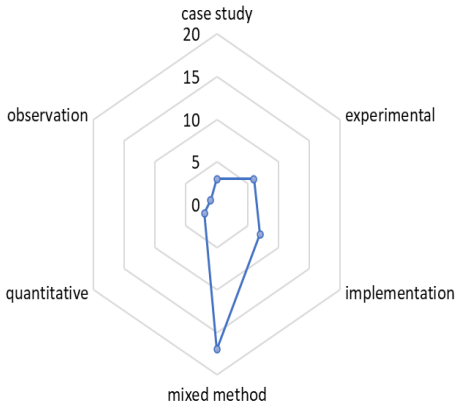

Figure 8. Commonly used research methods

The most notable technologies involved in the study area, as highlighted with the help of Figure 9, include mobile applications (n = 7), educational robots (n = 6), gamified applications (n = 4), video modeling (n = 4), augmented reality (n = 3), virtual reality (n = 3), educational multimedia (n = 3), maker program (n = 2), wearable devices (n = 2), web application (n = 2).

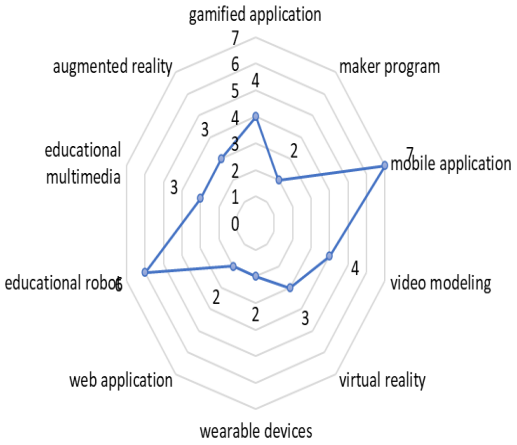

Figure 9. Commonly used technological interventions

3.2 Analysis of the Commonly Used Research Methodologies

The most prominent research designs utilized by previous studies to demonstrate the efficacy of various computer technologies in supporting ASD-inclusive education include case studies [25, 26, 37], experimental designs [8, 10, 12, 16, 20, 38], systems developments and implementations [15, 17, 21, 29, 30, 32, 47, 48], mixed study designs [19, 22-24, 27, 28, 33-36, 39-42, 49-51], observation [18] and quantitative research methodologies [7, 52]. Furthermore, the research methodologies were limited by small sample sizes and were mainly conducted in the US [7, 12, 25, 34, 35, 38-42, 50-52], and European countries [10, 15, 17, 26, 27, 32, 37]. Noteworthy, many relevant studies utilized small sample sizes, lacking long-term data and evidence of consensus with best ASD-inclusive practices. This could imply limited generalizability, lack of sustainability, and practical evidence. Therefore, apart from privacy and data security issues, future studies should propose cost-effective solutions, as some emerging technologies, such as VR and AR systems, could be expensive to implement in low- and middle-income countries and large educational settings.

Commented [E1]: According to the journal layout rule, references should be numbered in numerical order. Please add reference [47] in the main text and keep the reference number in numerical order.

Commented [ALA2]: Done. Thank you

3.3 Analysis of the Frequently Used Technological Interventions

The systematic literature search of the present study identified the most frequently employed emerging computer technologies for ASD-inclusive education, as shown with the help of Figure 9 and Table 1. Several studies aimed at supporting learners with ASD in inclusive settings using various technologies including mobile applications [7, 10, 12, 27-30], educational robots [8, 21-24, 49], gamified applications [25, 26, 48, 52], video modeling [37-40], augmented reality [18-20], virtual reality [15-17], educational multimedia [34-36], maker program [50, 51], wearable devices [41, 42], and web applications [32, 33]. Future studies must revisit the efficacy of the existing technological interventions and propose practical enhancements to provide sustainable strategies for ASD-inclusive education in evolving societies.

IV. DISCUSSION

4.1 Applications of Blockchain in Securing Defense and Critical Infrastructures

The integration of blockchain technology and cybersecurity in the military, defense, and protection of critical infrastructures is a pivotal area that has garnered significant attention. Recent studies highlighted various aspects of this integration, providing insights into its applications and benefits [1], [2], [3], [4], [25]. For instance, [2] introduced a Cognitive Radio Network (CRN) with blockchain technology as a solution for the Internet of Vehicles (IoV), recognizing the critical role of spectrum availability and the challenges posed by malicious devices, and preventing data alteration and enhance security during spectrum sensing and information transmission. The study findings from the proposed mechanism, validated through rigorous simulations, demonstrate significant efficiency gains in identifying malicious nodes and countering Denial of Service (DoS) threats compared to baseline solutions. Recently, [1] emphasized the importance of securing communication within the Battlefield of Things (BoT). The BoT, being integral to quick and precise decision-making in military operations, faces challenges such as data manipulation and breaches of privacy. The proposed blockchain-based solution addresses these concerns by ensuring both security and privacy within the BoT ecosystem. For critical infrastructures such as Air Traffic Management (ATM) Systems, nuclear plants, and industrial control systems, [3] proposed a comprehensive security architecture based on blockchain technology, establishing a distributed co-trust mechanism and multi-chain storage structure to provide systematic security assurance for the networked ATM system amid the dynamic and complex cyber-physical interactions. Similarly, [4] employed chimp optimization-based feature selection and optimal deep neural networks, coupled with a Blockchain-enabled integrity checking scheme (BEICS), to defend against misrouting attacks in critical infrastructures. The study findings indicated the effectiveness of BDLE-CAD, showcasing its superiority over existing techniques. Nonetheless, [26] explored the application of blockchain to enhance the cybersecurity of a Maritime Monitoring System (MMS). Deploying a blockchain solution, specifically HyperLedger Fabric, the study addresses scalability and cybersecurity challenges inherent in a nation-scale MMS. The practical experiment, incorporating a low-cost IoT setup, demonstrates the feasibility and effectiveness of the proposed blockchain-based solution, emphasizing its potential in ensuring the integrity, authenticity, and availability of navigation data in a maritime setting. [27] introduced a blockchain-based scheme. Employing zero-knowledge proof and commitment-based approaches, the proposed solution protects vessel identities and ensures relationship-related privacy during data trading. Security and performance evaluations validate the utility of the blockchain-based approach in facilitating accurate and private data sharing within large-scale deployments. In essence, the proposed solutions not only address specific challenges within their respective domains but also contribute to the broader discourse on leveraging blockchain to enhance the security and integrity of interconnected systems in these critical sectors. These studies highlighted the multifaceted applications of blockchain technology, showcasing its adaptability and efficacy in safeguarding sensitive information and critical operations.

4.2 Blockchain Solutions for Secured Healthcare Systems

The integration of blockchain technology into healthcare systems has emerged as a promising solution to address the vulnerabilities and security challenges associated with traditional as well as smart healthcare solutions. Accordingly, several studies highlighted various aspects of this intersection, presenting innovative frameworks and solutions that leverage blockchain for enhanced security in healthcare data management [5], [6], [7]. For instance, [5] proposed a lightweight private blockchain network to ensure the security and trustworthiness of healthcare operations by moving away from cloud-based architectures, which are susceptible to cyberattacks. The evaluation result of the framework demonstrates notable improvements in service execution time and throughput under different control parameters, reinforcing the efficacy of blockchain in ensuring the integrity of medical data. [6] proposed an AI-powered solution entitled BICS-AI which provides a high-security rate, performance, and success

rate, along with reduced latency compared to traditional IoT methods. The findings suggest that blockchain applications, particularly when combined with artificial intelligence, can offer a reliable means to identify and rectify potential life-threatening mistakes in the medical field. [28] proposed a cryptographic evidence-based framework that emphasized the importance of cryptographic proof in ensuring the security of medical data within smart healthcare systems. The implementation of smart contracts, backed by cryptographic proof, not only secures Electronic Health Records (EHRs) but also enables non-repudiation, enforceability, and accountability of digital agreements. The results of empirical tests and cybersecurity assessments of the study validate the effectiveness of the proposed framework, aligning with established methodologies such as those recommended by ENISA and NIST. [7] proposed a behavior-driven adaptive security framework entitled FBASHI framework to address the unique security challenges posed by IoT devices in healthcare by combining fuzzy logic and blockchain. FBASHI achieves Authentication, Authorization, and Audit Logs (AAA) services which are crucial for ensuring the security of healthcare IoT environments. The implementation using Hyperledger, a privacy-focused blockchain platform, demonstrates practicality and outperforms other blockchain-based solutions. Similarly, [29] proposed a privacy-preserving solution entitled BIoTHR that leverage blockchain and swarm exchange techniques to ensure seamless and secure transmission of Electronic Health Records (EHRs) across heterogeneous IoT networks. Simulation results of the study confirm the superiority of the proposed scheme in terms of blockchain-IoT integration and EHR transmission efficiency. In essence, the consensus among researchers regarding the transformative potential of blockchain technology in reinforcing cybersecurity within healthcare systems, based on the presented frameworks and solutions, showcased the versatility of blockchain applications in addressing specific challenges and significantly enhancing the security, integrity, and privacy of healthcare data. With continuous evolution in this direction, these advancements could pave the way for a more secure and resilient healthcare ecosystem.

4.3 Blockchain Solutions for Secured Industrial IoT

In recent years, the Industrial Internet of Things (IIoT) has emerged as a transformative force in various industrial sectors. Studies have shown the value of the integration of blockchain technology into IIoT frameworks as an effective strategy for addressing cybersecurity challenges [8], [9], [10]. For instance, [8] proposed a Blockchain-enabled Digital Twin Framework coupled with Deep Learning for early detection and prevention of botnet formation in Smart Factory environments, addressing the challenges posed by resource constraints in IIoT. The approach demonstrates privacy-preservation of data and prevent the participation of malicious nodes in botnet detection model training. Similarly, [9] presented a private blockchain architecture that utilizes a low-power ARM Cortex-M processor and employs proof of authentication (PoA) as a consensus mechanism to enhance security in an industrial application, specifically in a cement factory. Experimental results of the study highlight the achieved high levels of security, scalability, and ideal performance, showcasing the successful integration of blockchain technology with IIoT devices for efficient resistance against common cyber-security attacks. [10] introduced a novel Blockchain-based secure energy policy and load-sharing approach for renewable smart microgrids within the IIoT environment to safeguard against malicious cyber-attacks that could disrupt system performance, affecting parameters such as cost, environmental pollution, and unit output. The proposed policy prevents unauthorized manipulation of data, especially in the context of control layers organized in a master-slave (M-S) setting. [30] proposed a blockchain-enabled Threat Intelligence Integrity Audit (TIIA) scheme that employs a double-chain structure, utilizing a storage chain for threat intelligence ciphertext and an audit chain for integrity audit, ensuring confidentiality protection requirements on the blockchain. The proposed scheme demonstrates effectiveness in reducing computational and communication costs, providing a high level of audit efficiency in maintaining the integrity of threat intelligence on the blockchain.

4.4 Blockchain Solutions for Internet of Things (IoT) Security

Studies have showcased the fusion of blockchain with IoT, not only in enhancing the existing security configurations of IoT but also in introducing innovative solutions for secure, reliable, and privacy-preserving data management [31], [32], [33], [34], [35]. Notable examples include [31] in the proposed e-VoteD-App that integrates blockchain in an IoT-embedded e-voting system that ensures privacy and verifiability as well as anonymity which is crucial in democratic processes. Similarly, [32] leveraged blockchain, IPFS, and the PBFT consensus algorithm to enhance the security and traceability of firefighting IoT data storage. Results of the comparative analysis of the combined blockchain and IPFS technology highlighted the efficiency of the approach in reducing blockchain space overhead and ensuring IoT data security. The work of [33] demonstrated the application of blockchain in addressing the remote authentication challenges for IoT devices with potential contribution to the reliability and authenticity of electronic components. Nonetheless, [34] proposed a blockchain-

based authentication framework by combining blockchain technology with the modular square root algorithm. The result of experimental and security analysis of the framework achieves effective authentication that could address the concerns related to the heterogeneity and resource constraints of IoT devices. [19] presented a lightweight consortium blockchain architecture to facilitate intelligent autonomous access control for geographically dispersed, resource-constrained IoT devices. By storing access policies and authentication services on the blockchain, the system ensures reliability and confidentiality. Recently, [36] proposed a robust Token-Based Authorization and Authentication (TAA) mechanism to address cybersecurity concerns in Internet of Vehicles (IoV) communication. Leveraging blockchain technology and random forest machine learning techniques, the TAA method ensures secure information exchange in dynamic mobile city environments. Notably, the integration of blockchain-based authorization aids in updating specific token fields, thereby reducing vehicle-to-vehicle losses. The simulation results, considering variations in vehicle density, error rate, and classification sets, confirmed the effectiveness of the proposed approach in maximizing seamlessness while maintaining security. Similarly, [37] highlighted the vulnerability of IoT devices to cyber-attacks, and investigated the synergy of machine learning and blockchain in building an Intrusion Detection System (IDS). Accordingly, by encrypting interactions between IoT devices, blockchain contributes to a tamper-proof decentralized communication system. The incorporation of machine learning algorithms, particularly Random Forest, yields a remarkable detection accuracy of 99.9%, showcasing the efficacy of this integrated approach in fortifying the security and privacy of IoT networks.

4.5 Blockchain Solutions for Secured Smart Cities

Studies have highlighted multifaceted applications of blockchain in enhancing the security, integrity, and efficiency of various aspects associated with urban ecosystems based on smart city solutions [11], [12], [13], [38]. For instance, [11] emphasized the critical role of cybersecurity in smart cities and the attention it has attracted in recent years. The study proposed a comprehensive framework and architecture that leverages blockchain, big data, and artificial intelligence to demonstrate the promising potential for reinforcing smart city cybersecurity. The simulation results of the study, based on a smart grid dataset, provide compelling evidence of the effectiveness of the proposed framework in a real-world context. This reinforces the potential of blockchain to augment the security structure of smart cities by ensuring data security and confidentiality. Equally, [12] addressed the risks associated with cyber-attacks on IoT devices within smart cities. This study presented a novel framework, integrating blockchain with digital forensics with the aim of preserving digital evidence in a secure and tamper-proof manner. The proposed Forensics Chain for Evidence Preservation System leverages blockchain to guarantee the immutability and data integrity of preserved evidence. Thus, by distributing the digital evidence among forensic participant nodes, the framework mitigates the risks of single points of failure and unauthorized access. [13] focused on energy management within smart cities by demonstrating a secure management framework that incorporates blockchain technology. The study highlighted a novel integration of vehicle-to-subway (V2S) and vehicle-to-grid (V2G) concepts for optimal energy scheduling and operation. The proposed stochastic architecture of the study, utilizing unscented transformation (UT) to handle operational uncertainties, ensures the secure collaboration of all sub-systems within smart cities. Blockchain is deployed in the study to guarantee the security of data transfer, fostering a secure and integrated management structure. Consequently, the simulation results of the study confirmed the robustness of the proposed model in addressing the challenges of energy management in smart cities while highlighting the pivotal role of blockchain in securing data transfer mechanisms.

4.6 Blockchain Solutions for Secured Energy Systems

The growing reliance on digital infrastructure makes modern power grids susceptible to cyberattacks. A secured grid can withstand and rapidly recover from disruptions, minimizing the impact on consumers and the economy. Several studies have shown the transformative impact of blockchain in securing energy system infrastructure in addressing data tampering, decentralization for cost reduction, and enhanced anomaly detection among others [39], [40], [41], [42], [43], [44], [45]. For instance, [39] proposed a smart metering algorithm that utilizes blockchain to address the pressing issue of data tampering in smart meters, The proposed proof-of-efficiency consensus algorithm showcases improved performance in addressing storage and processing challenges with enhanced data security, establishing the efficacy of blockchain in fortifying smart metering applications. Similarly, [40] demonstrated the role of blockchain in secure data aggregation and power dispatching within decentralized and distributed power systems. Leveraging homomorphic encryption and the PBFT consensus, the proposed solution ensures secure data handling and enables automatic power dispatching with the integration of the PSO algorithm and smart contracts. enables. Equally, [42] and [46] addressed privacy concerns in distributed electricity trading within smart grids while supporting efficient transactions in trading for Renewable Energy Certificates (RECs) and Distributed

Attribute-Based Signature (DABS) schemes, respectively. Recently, [43] and [41] proposed a lightweight blockchain-based model for threat detection with reduced computational and communication costs in terms of network latency. The proposed models incorporate secure user authentication, lightweight data encryption, quantum key distribution, and optimal user privacy management. The experimental results of the studies highlighted high accuracy rates, highlighting the efficacy of blockchain in providing a secure and robust solution for cybersecurity threats in smart grid networks. In addition, [44] introduced a collaborative metering system architecture for smart grids with blockchain to ensure data integrity and security, addressing challenges in managing wide-range metering networks. The proposed solution, combining legacy and new technologies, presents a unique and innovative approach to advancing advanced metering infrastructure (AMI) in smart grids. [47] integrated blockchain into cyber-physical systems to enhance resilience, with a specific focus on the power grid as a distributed industrial network. Resilience is crucial for the stability of system operations, and the study investigates innovative business models empowered by blockchain in the face of managerial and cybersecurity challenges. Employing a multi-level technical framework and a customized Proof of Stake consensus, the study indicated blockchain integration strategies. The case study evaluated the performance improvement and resilience of business models, particularly in detecting false data injection attacks. In addition, the study results highlighted the potential of blockchain to provide constant validation and a consistent view of the system state in cyber-physical systems, contributing to the stability and security of critical infrastructures.

4.7 Blockchain Solutions for Secured Communication, Networking, and Smart Mobility

Several studies have demonstrated the efficacy of blockchain-based solutions in advancing the security of communication, networking, and smart mobility ecosystems [48], [49], [50], [51], [52]. For instance, exemplary integrations in the security of Vehicular Ad Hoc Networks (VANETs), [48] experimented with HCSC as a novel solution to the challenges faced in VANETs such as resource-constrained communication nodes, distributed geographical locations, and low delay requirements. HCSC is promising in addressing the opaque interaction and insufficient security verification of distributed authentication entities in VANETs by leveraging blockchain technology. Results of the experimental simulation and security analysis of the study demonstrated the efficiency and suitability of HCSC in managing key security challenges within VANETs. Equally, [49] provided analytical models and real-world experiments, based on the approaches for addressing the vulnerabilities associated with vehicle position-linked attacks in connected-vehicle fleets, to demonstrate the feasibility and benefits of real-time certificate revocation through the dynamic creation of vehicle communities and integration of blockchain technology. The proposed solution effectively mitigates Sybil and faking position attacks in V2X communications. The results suggest that real-time revocation through blockchain integration enhances the security of vehicular networks and meets the stringent real-time requirements of intelligent transport systems. Furthermore, [50] conducted a case study on Blockchain for the Smart Mobility Data Market (BSMD) as a multi-layered framework to address privacy, security, management, and scalability challenges associated with smart mobility data. BSMD is shown to secure the transaction of information by sharing encrypted data on a blockchain network. The principles of data ownership, transparency, auditability, and access control are emphasized, showcasing how blockchain can ensure cybersecurity and privacy in real-time mobility data-sharing scenarios. In addition, the BSMD framework demonstrates its performance on a 370-node blockchain running on heterogeneous and geographically separated devices. Similarly, [51] presented a risk assessment framework for blockchain applications in smart mobility, with a focus on quantifying risk associated with the multi-layered BSMD. Particularly, by employing actor-based, scenario-based, and combined analyses, the framework systematically evaluates the impact, probability, and overall risk associated with potential cybersecurity failures and uncovers specific security vulnerabilities within the transportation ecosystem, providing valuable insights into different attack vectors. The study analysis reveals the highest risk factors concerning monetary, privacy, integrity, and trust impacts on victims. In essence, the proposed framework offers a systematic approach to understanding and addressing cybersecurity risks in the integration of blockchain technologies within smart mobility.

V. CONCLUSION

The present study explored the transformative potential of blockchain technology in enhancing cybersecurity solutions across various application domains. The study provides a critical appraisal of the recent literature on the efficacy of blockchain's secure, transparent, and decentralized mechanisms for cybersecurity, thereby strengthening critical systems, safeguarding sensitive information, and enabling a more secure digital ecosystem. Firstly, studies on cybersecurity modalities in defense and critical infrastructures, have demonstrated the

multifaceted applications of blockchain, ranging from securing communication within military operations to safeguarding critical infrastructures such as air traffic management systems and nuclear plants. Blockchain-based solutions have been demonstrated to mitigate challenges posed by malicious activities, data manipulation, and breaches of privacy, thereby enhancing the resilience of interconnected systems in these pivotal domains. Secondly, within healthcare systems, recent studies have indicated the blockchain emergence as a promising tool for addressing security vulnerabilities inherent in traditional and smart healthcare solutions. By ensuring the integrity and trustworthiness of medical data, blockchain-based frameworks offer a reliable means to identify and rectify potential life-threatening mistakes while preserving patient privacy and confidentiality. Thirdly, in the context of industrial IoT, studies have shown the efficacy of blockchain solutions in enhancing cybersecurity measures within smart factory environments, and smart industrial infrastructure. Through innovative approaches such as blockchain-enabled digital twin frameworks and secure energy policy architectures, studies have integrated blockchain to reinforce data integrity and prevent unauthorized manipulation, thereby ensuring the secure operation of industrial systems. Fourthly, the integration of blockchain with IoT technologies has yielded innovative solutions for securing IoT networks and data management. Stem of studies from privacy-preserving e-voting systems to implementing lightweight consortium blockchain architectures for intelligent autonomous access control, proposed blockchain-based frameworks with robust mechanisms for ensuring the security and privacy of IoT ecosystems, even in resource-constrained environments. Fifthly, in the domain of smart cities, blockchain has been instrumental in enhancing the security, integrity, and efficiency of urban ecosystems. By leveraging blockchain, big data, and artificial intelligence, studies have presented comprehensive frameworks to reinforce smart city cybersecurity, preserve digital evidence, and optimize energy management processes, thereby advancing a secure and integrated urban infrastructure. Lastly, in the energy sector, studies have shown how blockchain emerges as a key enabler for securing power grid infrastructures and addressing cybersecurity threats. From smart metering techniques to collaborative metering system architectures, blockchain solutions offer enhanced data security, decentralized transaction mechanisms, and robust anomaly detection capabilities, ensuring the resilience and reliability of energy systems in the face of evolving cyber threats.

REFERENCES

[1] G. Sharma, D. K. Sharma, and A. Kumar, "Role of cybersecurity and Blockchain in battlefield of things," Internet Technol. Lett., vol. 6, no. 3, May 2023, doi: 10.1002/itl2.406.

[2] G. Rathee, F. Ahmad, F. Kurugollu, M. A. Azad, R. Iqbal, and M. Imran, "CRT-BIoV: A Cognitive Radio Technique for Blockchain-Enabled Internet of Vehicles," IEEE Trans. Intell. Transp. Syst., vol. 22, no. 7, pp. 4005–4015, Jul. 2021, doi: 10.1109/TITS.2020.3004718.

[3] X. Lu, R. Dong, Q. Wang, L. Zhang, R. Dick, and R. Dick, "Information Security Architecture Design for Cyber-Physical Integration System of Air Traffic Management," 2023.

[4] M. Ragab and A. Altalbe, "A Blockchain-Based Architecture for Enabling Cybersecurity in the Internet-of-Critical Infrastructures," 2022, doi: 10.32604/cmc.2022.025828.

[5] M. A. Khan, S. A. Alsuhibany, W. El-shafai, and M. U. Rehman, "An Immutable Framework for Smart Healthcare Using Blockchain Technology," 2023, doi: 10.32604/csse.2023.035066.

[6] M. Alshehri, "Blockchain-assisted cyber security in medical things using artificial intelligence," vol. 31, no. 2, pp. 708–728, 2022.

[7] Z. Zulkifl, F. Khan, and S. Member, "FBASHI : Fuzzy and Blockchain-Based Adaptive Security for Healthcare IoTs," vol. 10, 2022.

[8] M. M. Salim, J. H. Park, A. K. Comivi, T. Nurbek, and H. Park, "A Blockchain-Enabled Secure Digital Twin Framework for Early Botnet Detection in IIoT Environment," 2022.

[9] S. M. Umran, S. Lu, Z. A. Abduljabbar, J. Zhu, and J. Wu, "applied sciences Secure Data of Industrial Internet of Things in a Cement Factory Based on a Blockchain Technology," 2021.

[10] W. Xu, J. Li, M. Dehghani, and M. GhasemiGarpachi, "Blockchain-based secure energy policy and management of renewable-based smart microgrids," Sustain. Cities Soc., vol. 72, p. 103010, Sep. 2021, doi: 10.1016/j.scs.2021.103010.

[11] A. E. L. Bekkali and M. Essaaidi, "A Blockchain-Based Architecture and Framework for Cybersecure Smart Cities," no. July, pp. 76359–76370, 2023.

[12] R. Kamal, E. E. Hemdan, and N. El‐Fishway, "Forensics chain for evidence preservation system: An evidence preservation forensics framework for internet of things‐based smart city security using blockchain," Concurr. Comput. Pract. Exp., vol. 34, no. 21, Sep. 2022, doi: 10.1002/cpe.7062.

[13] L. Zhang, L. Cheng, F. Alsokhiry, and M. A. Mohamed, "A Novel Stochastic Blockchain-Based Energy Management in Smart Cities Using V2S and V2G," IEEE Trans. Intell. Transp. Syst., vol. 24, no. 1, pp. 915–922, 2023, doi: 10.1109/TITS.2022.3143146.

[14] H. Echchaoui, A. Ferdenache, and R. Boudour, "Introduction to Cybersecurity Applications in Blockchain Technology," Signals Commun. Technol., vol. Part F2318, pp. 3–28, 2024, doi: 10.1007/978-3-031-50733-5_1.

[15] Y. Maleh, S. Mounir, and K. Ouazzane, "Cybersecurity-Based Blockchain for Cyber-Physical Systems: Challenges and Applications," Adv. Inf. Secur., vol. 102, pp. 47–71, 2023, doi: 10.1007/978-3-031-25506-9_3.

[16] P. Asuquo, C. Ogah, W. Hathal, and S. Bao, "Blockchain Meets Cybersecurity: Security, Privacy, Challenges, and Opportunity," Stud. Big Data, vol. 60, pp. 115–127, 2020, doi: 10.1007/978-981-13-8775-3_5.

[17] V. H. Z. Tun and H. Jahankhani, "Using Artificial Intelligence (AI) and Blockchain to Secure Smart Cities' Services and Applications," Adv. Sci. Technol. Secur. Appl., vol. Part F2564, pp. 163–184, 2024, doi: 10.1007/978-3-031-52272-7_7.

[18] X. Zhu, "Consensus Algorithms in Blockchain : A survey to create decision trees for blockchain applications," 2023, [Online]. Available: https://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-329595

[19] X. Hao, W. Ren, Y. Fei, T. Zhu, and K. K. R. Choo, "A Blockchain-Based Cross-Domain and Autonomous Access Control Scheme for Internet of Things," IEEE Trans. Serv. Comput., vol. 16, no. 2, pp. 773–786, 2023, doi: 10.1109/TSC.2022.3179727.

[20] J.-C. Cheng, N.-Y. Lee, C. Chi, and Y.-H. Chen, "Blockchain and smart contract for digital certificate," in 2018 IEEE International Conference on Applied System Invention (ICASI), IEEE, Apr. 2018, pp. 1046–1051. doi: 10.1109/ICASI.2018.8394455.

[21] M. Aljohani, R. Mukkamala, and S. Olariu, "A Smart Contract-based Decentralized Marketplace System to Promote Reviewer Anonymity," in 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), IEEE, May 2023, pp. 524–532. doi: 10.1109/ICBC56567.2023.10175001.

[22] U. K. Shakila and S. Sultana, "A Decentralized Marketplace Application based on Ethereum Smart Contract," in 2021 24th International Conference on Computer and Information Technology (ICCIT), IEEE, Dec. 2021, pp. 1–5. doi: 10.1109/ICCIT54785.2021.9689879.

[23] R. Prakash, V. S. Anoop, and S. Asharaf, "Blockchain technology for cybersecurity: A text mining literature analysis," Int. J. Inf. Manag. Data Insights, vol. 2, no. 2, p. 100112, Nov. 2022, doi: 10.1016/j.jjimei.2022.100112.

[24] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, and T. P. Group, "Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement," PLoS Med., vol. 6, no. 7, p. e1000097, 2009, doi: 10.1371/journal.pmed.1000097.

[25] Y. Wang, P. Chen, B. Wu, C. Wan, and Z. Yang, "A trustable architecture over blockchain to facilitate maritime administration for MASS systems," Reliab. Eng. Syst. Saf., vol. 219, no. October 2021, p. 108246, 2022, doi: 10.1016/j.ress.2021.108246.

[26] U. Blockchain, L. I. Technology, and A. O. De Sá, "Towards a Secure and Scalable Maritime Monitoring System Using Blockchain and Low-Cost IoT Technology †," pp. 1–20, 2022.

[27] K. Gai et al., "Blockchain-Based Privacy-Preserving Positioning Data Sharing for IoT-Enabled Maritime Transportation Systems," IEEE Trans. Intell. Transp. Syst., vol. 24, no. 2, pp. 2344–2358, 2023, doi: 10.1109/TITS.2022.3190487.

[28] H. Szczepaniuk and E. K. Szczepaniuk, "Cryptographic evidence-based cybersecurity for smart healthcare systems," Inf. Sci. (Ny)., vol. 649, no. August, p. 119633, Nov. 2023, doi: 10.1016/j.ins.2023.119633.

[29] P. P. Ray, B. Chowhan, N. Kumar, and A. Almogren, "BIoTHR: Electronic Health Record Servicing Scheme in IoT-Blockchain Ecosystem," IEEE Internet Things J., vol. 8, no. 13, pp. 10857–10872, Jul. 2021, doi: 10.1109/JIOT.2021.3050703.

[30] W. Zhang, Y. Bai, and J. Feng, "TIIA: A blockchain-enabled Threat Intelligence Integrity Audit scheme for IIoT," Futur. Gener. Comput. Syst., vol. 132, pp. 254–265, Jul. 2022, doi: 10.1016/j.future.2022.02.023.

[31] C. Toma, M. Popa, C. Boja, and C. Ciurea, "Secure and Anonymous Voting D-App with IoT Embedded Device Using Blockchain Technology," 2022.

[32] L. Li, "A Secure , Reliable and Low-Cost Distributed Storage Scheme Based on Blockchain and IPFS for Firefighting IoT Data," IEEE Access, vol. 11, no. August, pp. 97318–97330, 2023, doi: 10.1109/ACCESS.2023.3311712.

[33] A. Augusto, N. Campos, and T. C. Pimenta, "Authentication for Integrated Circuit and Devices Using Blockchain and Physical Unclonable Functions," vol. 17, pp. 1–11, 2022.

[34] X. Yang, X. Yang, X. Yi, I. Khalil, X. Zhou, and D. He, "Blockchain-Based Secure and Lightweight Authentication for Internet of Things," no. May 2023, 2021, doi: 10.1109/JIOT.2021.3098007.

[35] S. Abbas, N. Javaid, S. Member, A. Ahmed, A. Radwan, and S. Member, "Securing Genetic Algorithm Enabled SDN Routing for Blockchain Based Internet of Things," IEEE Access, vol. 9, pp. 139739–139754, 2021, doi: 10.1109/ACCESS.2021.3118948.

[36] G. Manogaran, B. S. Rawal, V. Saravanan, M. K. Priyan, Q. Xin, and P. Shakeel, "Token-Based Authorization and Authentication for Secure Internet of Vehicles Communication," ACM Trans. Internet Technol., vol. 22, no. 4, Mar. 2023, doi: 10.1145/3491202.

[37] N. A. Alsharif, S. Mishra, and M. Alshehri, "IDS in IoT using Machine Learning and Blockchain," Eng. Technol. Appl. Sci. Res., vol. 13, no. 4, pp. 11197–11203, 2023, doi: 10.48084/etasr.5992.

[38] S. Mishra and V. K. Chaurasiya, "Hybrid deep learning algorithm for smart cities security enhancement through blockchain and internet of things," Multimed. Tools Appl., vol. 83, no. 8, pp. 22609–22637, Mar. 2024, doi: 10.1007/S11042-023-16406-6/METRICS.

[39] J. C. Olivares-Rojas, E. Reyes-Archundia, J. A. Gutierrez-Gnecchi, J. Cerda-Jacobo, and J. W. Gonzalez-Murueta, "A Novel Multitier Blockchain Architecture to Protect Data in Smart Metering Systems," IEEE Trans. Eng. Manag., vol. 67, no. 4, pp. 1271–1284, 2020, doi: 10.1109/TEM.2019.2950410.

[40] X. Luo, K. Xue, J. Xu, Q. Sun, and Y. Zhang, "Blockchain Based Secure Data Aggregation and Distributed Power Dispatching for Microgrids," IEEE Trans. Smart Grid, vol. 12, no. 6, pp. 5268–5279, 2021, doi: 10.1109/TSG.2021.3099347.

[41] S. Nasiri, H. Seifi, and H. Delkhosh, "A Secure Power System Distributed State Estimation via a Consensus-Based Mechanism and a Cooperative Trust Management Strategy," IEEE Trans. Ind. Informatics, vol. 20, no. 2, pp. 3002–3014, 2023, doi: 10.1109/TII.2023.3299385.

[42] U. Cali, M. Kuzlu, D. J. Sebastian-Cardenas, O. Elma, M. Pipattanasomporn, and R. Reddi, "Cybersecure and scalable, token-based renewable energy certificate framework using blockchain-enabled trading platform," Electr. Eng., 2022, doi: 10.1007/s00202-022-01688-0.

[43] S. Mishra, "Blockchain-based security in smart grid network," Int. J. Commun. Networks Distrib. Syst., vol. 28, no. 4, pp. 365–388, 2022, doi: 10.1504/IJCNDS.2022.123863.

[44] E. Zanghi, M. Brown Do Coutto Filho, and J. C. Stacchini de Souza, "Collaborative smart energy metering system inspired by blockchain technology," Int. J. Innov. Sci., vol. 16, no. 2, pp. 227–243, Feb. 2023, doi: 10.1108/IJIS-07-2022-0127/FULL/XML.

[45] B. Wang, M. Dabbaghjamanesh, A. Kavousi-Fard, and S. Mehraeen, "Cybersecurity Enhancement of Power Trading within the Networked Microgrids Based on Blockchain and Directed Acyclic Graph Approach," IEEE Trans. Ind. Appl., vol. 55, no. 6, pp. 7300–7309, 2019, doi: 10.1109/TIA.2019.2919820.

[46] Q. Su, R. Zhang, R. Xue, Y. Sun, and S. Gao, "Distributed Attribute-Based Signature with Attribute Dynamic Update for Smart Grid," IEEE Trans. Ind. Informatics, vol. 19, no. 9, pp. 9424–9435, 2023, doi: 10.1109/TII.2022.3228688.

[47] X. Liang, C. Konstantinou, S. Shetty, E. Bandara, and R. Sun, "Decentralizing Cyber Physical Systems for Resilience: An Innovative Case Study from A Cybersecurity Perspective," Comput. Secur., vol. 124, p. 102953, Jan. 2023, doi: 10.1016/j.cose.2022.102953.

[48] Q. Zhu, A. Jing, C. Gan, X. Guan, and Y. Qin, "HCSC: A Hierarchical Certificate Service Chain Based on Reputation for VANETs," IEEE Trans. Intell. Transp. Syst., vol. 24, no. 6, pp. 6123–6145, 2023, doi: 10.1109/TITS.2023.3250279.

[49] A. Didouh, H. Labiod, Y. El Hillali, and A. Rivenq, "Blockchain-Based Collaborative Certificate Revocation Systems Using Clustering," IEEE Access, vol. 10, pp. 51487–51500, 2022, doi: 10.1109/ACCESS.2022.3160171.

[50] D. López and B. Farooq, "A multi-layered blockchain framework for smart mobility data-markets," Transp. Res. Part C Emerg. Technol., vol. 111, pp. 588–615, Feb. 2020, doi: 10.1016/j.trc.2020.01.002.

[51] R. Al Mallah, D. Lopez, and B. Farooq, "Cyber-Security Risk Assessment Framework for Blockchains in Smart Mobility," IEEE Open J. Intell. Transp. Syst., vol. 2, no. June, pp. 294–311, 2021, doi: 10.1109/OJITS.2021.3106863.

[52] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K. K. R. Choo, "Blockchain-Based Cross-Domain Authentication for Intelligent 5G-Enabled Internet of Drones," IEEE Internet Things J., vol. 9, no. 8, pp. 6224–6238, Apr. 2022, doi: 10.1109/JIOT.2021.3113321.