Promises, Challenges and Opportunities of Integrating SDN and Blockchain with IoT Applications: A Survey

Loubna Elhaloui[1], Mohamed Tabaa[2], Sanaa Elfilali[3], El habib Benlahmar[4]
Pluridisciplinary Laboratory of Research and Innovation (LPRI), EMSI Casablanca, Casablanca, Morocco[1, 2]
Laboratory of Information Technologies and Modelling-Faculty of Sciences Ben M'sik,
Hassan II University, Casablanca, Morocco[1, 3, 4]

***Abstract*—Security is a major issue in the IT world, and its aim is to maintain user confidence and the coherence of the entire information system. Various international and European research projects, as well as IT manufacturers, have proposed new solutions and mechanisms to solve the problem of security in the IoT environment. Software-Defined Networking (SDN) and Blockchain are advanced technologies utilized globally for establishing secure network communication and constructing resilient network infrastructures. They serve as a robust and dependable foundation for addressing various challenges, including security, privacy, scalability, and access control. Indeed, SDN and Blockchain technologies have demonstrated their ability to efficiently manage resource utilization and facilitate secure network communication within the Internet of Things (IoT) ecosystem. Nonetheless, there exists a research gap concerning the creation of a comprehensive framework that can fulfill the unique requirements of the IoT environment. Consequently, this paper presents a recent investigation into the integration of SDN and Blockchain with IoT. The objective is to analyze their primary contributions and identify the challenges involved. Subsequently, we offer relevant recommendations to address these challenges and enhance the security and privacy of the IoT landscape.**

***Keywords*—Internet of things; SDN; blockchain**

I. INTRODUCTION

The Internet of Things (IoT) paradigm is shaping the future of computing, rapidly integrating into our daily lives to enhance our quality of life by connecting various smart devices, technologies, services, and applications [1]. Nonetheless, managing IoT networks poses several challenges that demand innovative solutions. These challenges primarily revolve around the inherent vulnerabilities of IoT devices, including susceptibility to outages, failures under heavy traffic loads, security vulnerabilities, limited energy efficiency, and scalability issues. Given the heterogeneity and resource constraints of IoT devices, they require specialized network behaviors and services, such as security protocols, efficient power management, and load balancing modules.

Software-Defined Networking (SDN), with its novel network management approaches and recent advancements in the IoT domain, offers promising solutions. It grants global visibility into network status and enables logically centralized resource control, which can be physically distributed as needed via programmable APIs from a central point [2]. Consequently, SDN facilitates the implementation of innovative network management techniques. Consequently, considerable research efforts are dedicated to developing SDN-based IoT management frameworks [3]. While SDN lays the groundwork for robust management solutions, the integration of intelligent decision-making in uncertain scenarios is still lacking, necessitating the incorporation of AI-based approaches alongside SDN.

Blockchain and IoT are both innovations that can bring significant advantages to IoT networks, such as improved security, transparency, immutability, privacy, and automated business processes. However, when combined within an SDN framework for IoT network management, the potential benefits of these technologies are further amplified. Looking ahead, we envision the introduction of adaptive resource management frameworks for IoT networks with the assistance of AI, which will also incorporate blockchain-based SDN frameworks. Furthermore, as IoT is expected to undergo large-scale deployment in the future, practical challenges that go beyond controlled laboratory settings or theoretical assessments will emerge. The current state of research in this field suggests that the dynamic capabilities offered by SDN can be leveraged to reconfigure, update, and enhance IoT networks in real-time to address emerging challenges.

Despite the many advantages mentioned above, the integration of new emerging technologies into the security of information and communication systems can give rise to a number of problems. Critical situations, in particular, raise further questions. Since the integration of Blockchain and SDN into the Internet of Things (IoT) is a dynamic process influenced by several interdependent factors, the addition of Blockchain to the IoT ecosystem intensifies technological and organizational requirements. As such, this paper aims to present an in-depth study of the challenges associated with IoT integration. Consequently, attention is specifically focused on the following research questions:

RQ1: What current challenges hinder the integration of Blockchain and SDN technologies into the IoT?

RQ2: What guidance does the literature provide to surmount these challenges?

This paper offers several significant contributions. Firstly, despite the use of Blockchain in recent years, there is a lack of in-depth research into the challenges of the Internet of Things (IoT). This study proposes a comparative study of IoT security solutions, based on existing literature relating to its integration. The paper explores the current problems of decentralizing the IoT with Blockchain, as well as future challenges in this field.

The paper's structure is outlined as follows: In Section II, we delve into related work that is pertinent to our paper. Following that, in Section III, we present a comprehensive comparative analysis of technological solutions aimed at enhancing IoT security. Section IV is dedicated to the discussion of our findings and the presentation of results. Ultimately, the paper wraps up with a conclusion in Section V.

II. Related Work

A. Internet of Things with SDN

The authors in [4] examined the Manufacturer's Use Description (MUD) model, which encompasses network access control, data privacy, as well as policies for channel and authorization protection. They employed an SDN platform to efficiently access device data and resources and utilized Blockchain technology, specifically Hyperledger, for sharing data among IoT devices. Additionally, Molina and colleagues in [5] introduced a security framework for the continuous, on-demand management of virtual authentication, authorization, and accounting (AAA) in SDN-enabled IoT networks. Their work achieved scalable bootstrapping of IoT devices and fine-grained management of network access control.

Moreover, the authors in [6] introduced a novel combination of cloud computing, IoT, and SDN, resulting in the CENSOR framework. This framework was designed to establish a secure gateway within the IoT environment, featuring a reliable and secure IoT network architecture powered by cloud computing and based on SDN technology. The authors also highlighted several challenges and potential threats that need to be addressed, including advanced security measures to counter Distributed Denial of Ser-vice (DDoS) attacks, appropriate routing algorithms, and network scalability.

The authors in [7] proposed the use of a distributed controller cluster to address is-sues related to reliability, scalability, fault tolerance, and interoperability in an SDN network. Their method was found to maintain reasonable CPU utilization, thus optimizing controller performance, with a particular focus on enhancing the security of IoT applications.

Lastly, the authors in [8] introduced Middlebox-Guard (M-G), an SDN-based model for enhancing data transfer security in response to various attacks and to improve network stability. They first addressed the placement of middleboxes, which are associated with predefined security policies, using a placement selection algorithm. Subsequently, two SDN resource control algorithms were employed to fulfill coverage requirements within switching volume constraints. Simulation results demonstrated that the M-G model they designed could effectively enhance the security and stability of IoT networks.

B. Internet of Things with Blockchain

Cryptocurrency and financial transactions initially introduced blockchain technology, wherein all nodes within the blockchain execute and store all transactions. Blockchain, with its versatility, finds application in various domains, one of the most prominent being the Internet of Things (IoT) [9]. The IoT consists of networks of intelligent devices like Raspberry Pi, ESP, etc., which interconnect seamlessly to form a network used for sensing, processing, and communication. These smart IoT devices operate autonomously, consuming minimal energy and possessing lightweight characteristics. According to Statista Com [10], the estimated number of IoT devices in 2020 stood at 31 billion globally, and this number is projected to reach 75 billion devices by the end of 2025 [11].

In the IoT context, smart devices are primarily dedicated to energy-intensive tasks related to vital applications, making the implementation of privacy and security measures challenging. Malicious attacks can disrupt IoT services and pose threats to user privacy, data security, and overall network confidentiality [12]. These attacks in IoT-based systems fall into four main categories: physical attack, network attack, soft-ware attack, and data attack [13].

Physical Attack: In this category, attackers are physically close to the network and attempt to carry out malicious activities through various means, such as manipulating IoT devices, blocking RF signals, injecting malicious code, and conducting side-channel attacks. One countermeasure involves the use of physical non-clonable functions (PUF) to authenticate IoT devices, as it prevents physical attacks [14]. PUFs have a unique feature that makes it impossible to replicate the precise microstructure of an IoT device.

Network Attack: Attackers in this category seek to manipulate the IoT network through methods like RFID spoofing, man-in-the-middle attacks, traffic analysis, and Sybil attacks. Preventative measures include authentication techniques and secure hash functions [15].

Software Attack: Attackers exploit vulnerabilities in the current software of IoT systems.

Data Attack: This category involves unauthorized data access and data inconsistency. To thwart such attacks, blockchain technology can be used to provide effective privacy-preserving mechanisms [16].

Furthermore, several studies have proposed solutions to enhance IoT security:

In study [17], an algorithm secures the externalizations of bilinear pairings of IoT devices, significantly improving performance compared to standard bilinear matching.

The authors in [18] presents a framework based on a hybrid blockchain approach to secure multinational-level Industrial Internet of Things (IIoT) deployments across multiple countries.

In research [19], a patient-centric blockchain framework addresses data protection, authentication, and immutability concerns, built on the Hyperledger platform.

In study [20] proposes an Ethereum-based smart contract platform for a blockchain-driven healthcare infrastructure, offering potential efficiency improvements in hospital settings.

Lastly, in study [21] introduces an approach utilizing an open-source blockchain (Ethereum) to secure the outsourcing of bilinear pairs in IoT systems, addressing limitations of centralization and validating its effectiveness in securing IoT applications.

C. Blockchain and SDN for the Internet of Things

This section addresses the two research questions (RQ1: What current challenges hinder the integration of Blockchain and SDN technologies into the IoT? RQ2: What guidance does the literature provide to surmount these challenges?) We consulted the relevant literature for answers to the research questions. The search strategy encompassed the use of all well-known databases, including ACM digital library, Elsevier, IEEE and MDPI.

In their study [22], the authors introduced an innovative IoT architecture that effectively merges cutting-edge SDN and Blockchain technologies. The primary objective of this architecture is to integrate SDN controllers into IoT networks, utilizing a clustered structure along with a novel routing protocol to tackle various network challenges including security, privacy, access control, and availability. Their particular focus lies in devising energy-efficient mechanisms for data transfer among IoT devices within the SDN framework. This architecture harnesses both public and private blockchains to facilitate peer-to-peer communication between IoT devices and SDN controllers, incorporating a distributed trust authentication method.

Similarly, Chaudhary and colleagues [23] harnessed blockchain and SDN technologies to enhance the quality of service in an intelligent transportation system. They designed BEST, a blockchain-based secure energy exchange system for electric vehicles. BEST employs blockchain for decentralized validation of vehicle requests, thus eliminating single points of failure. Simulation results demonstrated the successful integration of blockchain into the SDN architecture, resulting in improved network QoS and more efficient energy usage, although it did not consider various energy sources.

The authors in [24] introduced Cochain-SC, a blockchain-based architecture that enables secure collaboration and decentralized attack information transfer among multiple SDN domains. This architecture combines intra-domain and inter-domain DDoS mitigation. The authors evaluated Cochain-SC's performance in terms of efficiency, security, cost-effectiveness, and the accuracy of detecting illegitimate flows.

Ferrag et al. [25] provided an extensive overview of Blockchain technology applications across various IoT domains, such as the Internet of Vehicles, the Internet of Energy, virtual web, cloud computing, and edge computing. Their study also addressed the five most common attacks in IoT networks, namely identity-based, cryptanalysis-based, reputation-based, manipulation-based, and service-based attacks. They established taxonomy of recent methods for achieving secure, privacy-preserving Blockchain technologies, comparing them based on specific models, security objectives, performance, computational complexity, limitations, and communication costs.

In study [26], the authors introduced the "DistBlockNet" framework, designed for a secure distributed SDN architecture for IoT through the use of Blockchain technology. They presented a scheme for updating and validating rule tables using Blockchain, with experimental evaluation demonstrating the effectiveness of DistBlockNet in terms of accuracy, scalability, defense capabilities, and performance overhead.

Blockchain technology, despite relying on a group of nodes that may not all be fully trustworthy, offers a dependable data structure thanks to its appropriate consensus algorithm. This makes it a valuable solution to address security challenges in IoT and SDN. In [27], decentralized security architecture based on SDN and block-chain for the IoT ecosystem was proposed, aiming to enhance attack detection and mitigation. Blockchain was employed for dynamic attack detection model updates and Fog node rewards based on proof-of-work.

Additionally, the authors in [28] introduced a blockchain-based controller designed to combat the injection of fake flow rules, primarily focusing on SDN controller authentication. The authors in [29] presented a novel blockchain-based authentication handover for an SDN-based 5G network, aiming to eliminate unnecessary reauthentication during repeated handovers between heterogeneous cells in 5G net-works.

Lastly, Qiu et al. [30] explored the Industrial Internet of Things scenario involving multiple SDN controllers. They proposed a blockchain-based consensus protocol for collecting and synchronizing network-wide views between different SDN controllers, employing the Q-learning method to optimize view switching, access selection, and computational resources.

In summary, various studies have proposed diverse solutions to integrate block-chain within an SDN-based IoT ecosystem. However, comprehensive scenarios that encompass all aspects of these works are yet to be fully developed.

III. Comparative Study of IoT Security Technology Solutions

The significance of combining blockchain and SDN with IoT has found application across a diverse range of domains. Table I highlights prevalent areas and recent research endeavors where the integration of blockchain and SDN with IoT applications plays a pivotal role. The majority of these studies are dedicated to enhancing security and privacy within the IoT landscape through the utilization of these two technologies. Notably, Table I reveals that these articles contend with specific challenges, notably in the realms of privacy and scalability.

TABLE I. RECENT STUDIES ON INTEGRATING BLOCKCHAIN AND SDN INTO THE IOT APPLICATIONS

Recent Survey Article	Years	Domain	IoT security	IoT privacy	Scalability	SDN-IoT	Blockchain
Oualha et al. [31]	2016	IoT device	√		√		
Mao et al. [32]	2016	IoT device	√				
Tonyali et al. [33]	2016	Smart Grid		√			
Hardjono et al. [34]	2016	IoT device	√		√		√
Hashemi et al. [35]	2016	IoT environment	√		√		√
Kokoris-K et al. [36]	2016	IoT device			√		√
Kamanashis et al. [37]	2016	Smart Cities	√		√		√
Bull et al. [38]	2016	IoT device	√			√	
Vandana et al. [39]	2016	IoT environment	√		√	√	
Gonzalez et al. [40]	2016	IoT environment	√		√	√	
Huh et al. [41]	2017	IoT device	√				√
Zhang and Wen [42]	2017	IoT E-business					√
Atlam et al. [43]	2020	IoT device					√
Khan and Salah [44]	2018	IoT System	√		√		√
Badr et al. [45]	2018	E-HEALTH	√	√			√
Uddin et al. [46]	2021	Cloud & Fog IoT					√
Dorri et al. [47]	2016	IoT System	√	√			√
Salman et al. [48]	2019	Cloud Computing	√	√			√
Dai et al. [49]	2019	Smart Industry	√				√
Zhang et al. [50]	2019	IoT System	√				
Lao et al. [51]	2021	IoT application					√
Patil et al. [52]	2018	Smart green house	√	√			√
Polyzos and Fotiou [53]	2017	IoT device	√				√
Zhu and Badr [54]	2018	IoT environment	√	√			
Mishra and Tyagi [55]	2019	E-HEALTH	√				√
Banerjee et al. [56]	2018	IoT SYSTEM	√				√
Wang et al. [57]	2019	IoT application	√				√
Sengupta et al. [58]	2020	Industrial IoT	√				√
Jesus et al. [59]	2018	IoT device	√	√			√
Dwivedi et al. [60]	2021	Industrial IoT					√
Kamilaris et al. [61]	2019	Smart Agriculture					√
Ferrag et al. [62]	2019	IoT Environment	√				
Zheng et al. [63]	2017	APPLICATION					√
Thakore et al. [64]	2019	IoT SYSTEM					√
Hassan et al. [65]	2019	IoT Application					√
Lin et al. [66]	2018	Smart Agriculture					√
Dogo et al. [67]	2019	Smart Agriculture	√				√
Kadam and John [68]	2020	IoT device	√	√			√
Maroufi et al. [69]	2019	IoT device					√
Alamri et al. [70]	2019	APPLICATION	√	√			√
Atlam and Wills [71]	2019	IoT device	√	√			
Saad et al. [72]	2019	IoT SYSTEM					√
Atlam et al. [73]	2019	IoT Environment	√				√
Tandon [74]	2019	APPLICATION	√	√			√
Karthikeyan et al. [75]	2019	APPLICATION		√			√
Fotiou et al. [76]	2018	Smart device	√	√			
Hang and Kim [77]	2019	IoT System	√	√			√
Mahmood et al. [78]	2021	IoT device	√				
R. Alcarria et al. [79]	2018	Smart Communities	√	√			√

Recent Survey Article	Years	Domain	IoT security	IoT privacy	Scalability	SDN-IoT	Blockchain
Oualha et al. [31]	2016	IoT device	√		√		
A. G. Ghandour [80]	2019	Smart City	√	√			√
A. Rahman [81]	2020	Smart Building	√	√	√	√	√
P. K. Sharma and J. H. Park [82]	2018	Smart City	√	√	√	√	√
Y. Gu, D. Hou [83]	2018	Cloud Computing	√	√			√
A. Yazdinejad [84]	2020	IoT Network	√	√	√	√	√
P. Singh [85]	2020	Smart City	√				√
P. K. Sharma [86]	2019	Smart Industry & Smart City	√	√	√		√
D. Sinh [87]	2018	Smart Network	√			√	
M. J. Islam [88]	2019	Smart City	√			√	
I. Abdulqadder [89]	2018	Cloud Environment				√	
R. Chaudhary [90]	2019	Smart Grid	√			√	√
P. K. Sharma [91]	2017	IoT Network	√			√	√
B. K. Mukherjee [92]	2020	Smart City	√			√	
A. Rahman [93]	2020	Smart Industry	√		√	√	√
A. Rahman [94]	2019	Smart City	√		√	√	√
Ali et al. [95]	2018	IoT Network	√	√	√	√	√
Alladi et al. [96]	2019	Smart Industry	√	√	√		√
Xie et al. [97]	2019	Smart City	√	√			√
Yang et al. [98]	2019	Edge Computing	√	√	√		√
Ahmed et al. [99]	2020	Smart City	√	√			√
Ferrag et al. [100]	2020	Smart Green agriculture	√		√		√
Wang et al. [101]	2020	Industrial IoT	√	√			√
Bhushan et al. [102]	2021	IoT Network	√		√		√
Majeed et al. [103]	2021	Smart City	√	√	√		√
Da Xu et al. [104]	2021	Edge Computing	√				√
Yaqoob et al. [105]	2021	E-health	√		√		√
Abdelmaboud et al. [106]	2022	IoT Application	√		√		√
Kumar et al. [107]	2022	Smart Industry	√	√			√
Yu et al. [108]	2022	Smart City	√				√
Pennino et al. [109]	2022	IoT Economy			√		√
Alkhateeb et al. [110]	2022	Hypride BC for IoT			√		

IV. DISCUSSION

After examining 80 articles, it became evident that 80% of them were centered on enhancing the security of the Internet of Things (IoT). Additionally, 37% of these articles concentrated on matters pertaining to IoT privacy, while 30% delved into the evolution of IoT security. Consequently, blockchain has emerged as a potent and actively utilized tool for delivering the proposed security services for IoT applications.

Our initial approach involved categorizing diverse IoT applications by identifying their specific security requirements and the challenges they inherently face. Subsequently, we explored IoT solutions that addressed aspects of confidentiality, privacy, and availability, drawing upon conventional methods. Furthermore, we introduced emerging technologies such as Software Defined Networking (SDN) and Blockchain, both recognized for their effectiveness in mitigating scalability issues within the IoT ecosystem.

Moreover, we dedicated attention to security solutions that take into account the contextual aspects inherent to IoT applications, as delineated in Table II. We also considered the varying impacts of security concerns on system safety, alongside the corresponding countermeasures. Throughout our exploration, we provided an extensive comparative analysis of the different approaches, grounded in specific criteria. We also conducted an examination of techniques suitable for different types of IoT applications.

Despite ongoing efforts to confront the myriad challenges confronting the Internet of Things, numerous issues remain unresolved, notably those related to scalability and dynamism. This is particularly pertinent as the IoT continues its evolution into an "Internet of Everything," where humans, data, processes, and objects coalesce within a highly dynamic and intricately interconnected system.

TABLE II. NUMBER OF RELATED ARTICLES RANKED BY SCOPE OF CONTRIBUTION

Scope of the literature	Number of articles
IoT security	62
IoT privacy	29
Scalability	24
SDN-IoT	16
Blockchain	63
IoT security with Blockchain	48
IoT privacy with Blockchain	25
IoT security with SDN and Blockchain	9

V. CONCLUSION

The Internet of Things (IoT) confronts an array of security issues that surpass the complexities encountered in other domains, primarily owing to its intricate ecosystem and the inherent limitations of resource-constrained IoT devices. In recent years, an extensive body of research has been dedicated to addressing the diverse security challenges intimately linked with the IoT landscape. These challenges encompass intricate aspects such as authentication, confidentiality, integrity, access control, and policy enforcement, among a multitude of others.

Predominantly, prior works in the literature have strived to adapt security solutions initially devised for wireless and Internet sensor networks to suit the specific demands of the IoT framework. Nonetheless, it is imperative to underscore that IoT challenges present a novel dimension that proves considerably arduous to surmount using conventional remedies. Furthermore, it is crucial to emphasize that a significant proportion of prevailing security methodologies are rooted in centralized architectures, rendering their application within the IoT context notably more intricate due to the sheer abundance of interconnected entities. Consequently, a shift towards distributed approaches is imperative to effectively address the multifaceted security challenges that the IoT inherently presents.

REFERENCES

[1] Burhan, Muhammad, Rehman, Rana Asif, Khan, Bilal, et al. IoT elements, layered architectures and security issues: A comprehensive survey. sensors, 2018, vol. 18, no 9, p. 2796.

[2] Elhaloui, Loubna, Tabaa, Mohammed, Elfilali, Sanaa, et al. Dynamic security of IoT network traffic using SDN. Procedia Computer Science, 2023, vol. 220, p. 356-363.

[3] Siddiqui, Shahbaz, Hameed, Sufian, Shah, Syed Attique, et al. Towards Software-Defined-Networking-based IoT: A Systematic Literature Review on Management Frameworks and Open Challenges. 2021.

[4] S. N. Matheu, A. R. Enciso, A. M. Zarca, D. Garcia-Carrillo, J. L. Hernández-Ramos, J. B. Bernabe, and A. F. Skarmeta, ``Security architecture for de_ning and enforcing security pro_les in DLT/SDN-based IoT systems," Sensors, vol. 20, no. 7, p. 1882, Mar. 2020.

[5] A. M. Zarca, D. Garcia-Carrillo, J. B. Bernabe, J. Ortiz, R. Marin-Perez, and A. Skarmeta, ``Enabling virtual AAA management in SDN-based IoT networks," Sensors, vol. 19, no. 2, p. 295, Jan. 2019.

[6] M. Conti, P. Kaliyar, and C. Lal, ``CENSOR: Cloud-enabled secure IoT architecture over SDN paradigm," Concurrency Comput., Pract. Exper., vol. 31, no. 8, p. e4978, Apr. 2019.

[7] A. Abdelaziz, A. T. Fong, A. Gani, U. Garba, S. Khan, A. Akhunzada, H. Talebian, and K.-K.-R. Choo, ``Distributed controller clustering in software de_ned networks," PLoS ONE, vol. 12, no. 4, Apr. 2017, Art. no. e0174715.

[8] Y. Liu, Y. Kuang, Y. Xiao, and G. Xu, ``SDN-based data transfer security for Internet of Things," IEEE Internet Things J., vol. 5, no. 1, pp. 257_268, Feb. 2018.

[9] H. F. Atlam and G. B. Wills, "IoT security, privacy, safety and ethics," in Internet of Things, Springer International Publishing, 2020, pp. 123–149.

[10] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: a systematic survey," Sensors, vol. 18, no. 8, Aug. 2018, doi: 10.3390/s18082575.

[11] M. H. Rehman, I. Yaqoob, K. Salah, M. Imran, P. P. Jayaraman, and C. Perera, "The role of big data analytics in industrial internet of things," Future Generation Computer Systems, vol. 99, pp. 247–259, Oct. 2019, doi: 10.1016/j.future.2019.04.020.

[12] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in IoT: challenges and solutionss," Blockchain: Research and Applications, vol. 2, no. 2, 2021, doi: 10.1016/j.bcra.2021.100006.

[13] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoTt," Journal of Network and Computer Applications, vol. 149, 2020, doi: 10.1016/j.jnca.2019.102481.

[14] K. Mahmood et al., "PUF enable lightweight key-exchange and mutual authentication protocol for multi-server based D2D communication," Journal of Information Security and Applications, vol. 61, Sep. 2021, doi: 10.1016/j.jisa.2021.102900.

[15] D. Mishra, P. Vijayakumar, V. Sureshkumar, R. Amin, S. H. Islam, and P. Gope, "Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks," Multimedia Tools and Applications, vol. 77, no. 14, pp. 18295–18325, Nov. 2018, doi: 10.1007/s11042-017-5376-4.

[16] S. K. Dwivedi, R. Amin, and S. Vollala, "Blockchain-based secured IPFS-enable event storage technique with authentication protocol in VANET," IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 12, pp. 1913–1922, Dec. 2021, doi: 10.1109/JAS.2021.1004225.

[17] Zhang, H.; Tong, L.; Yu, J.; Lin, J. Blockchain Aided Privacy-Preserving Outsourcing Algorithms of Bilinear Pairings for Internet of Things Devices. arXiv 2021, arXiv:2101.02341.

[18] Rathee, G.; Ahmad, F.; Sandhu, R.; Kerrache, C.A.; Azad, M.A. On the design and implementation of a secure blockchain-based hybrid framework for Industrial Internet-of-Things. Inf. Process. Manag. 2021, 58, 102526.

[19] Singh, A.P.; Pradhan, N.R.; Agnihotri, S.; Jhanjhi, N.; Verma, S.; Ghosh, U.; Roy, D. A Novel Patient-Centric Architectural Framework for Blockchain-Enabled Healthcare Applications. IEEE Trans. Ind. Inform. 2020, 17, 5779–5789.

[20] Latif, R.M.A.; Hussain, K.; Jhanjhi, N.; Nayyar, A.; Rizwan, O. A remix IDE: Smart contract-based framework for the healthcare sector by using Blockchain technology. Multimed. Tools Appl. 2020, 1–24.

[21] Lin, C.; He, D.; Huang, X.; Xie, X.; Choo, K.-K.R. Blockchain-based system for secure outsourcing of bilinear pairings. Inf. Sci. 2020, 527, 590–601.

[22] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K.-R. Choo, ``An energy-ef_cient SDN controller architecture for IoT networks with blockchain-based security," IEEE Trans. Services Comput., vol. 13, no. 4, pp. 625_638, Jul. 2020.

[23] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, and K.-K.-R. Choo, ``BEST: Blockchain-based secure energy trading in SDNenabled intelligent transportation system," Comput. Secur., vol. 85, pp. 288_299, Aug. 2019.

[24] Z. A. El Houda, A. S. Ha_d, and L. Khoukhi, ``Cochain-SC: An intra- and inter-domain ddos mitigation scheme based on blockchain using SDN and smart contract," IEEE Access, vol. 7, pp. 98893_98907, 2019.

[25] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, ``Blockchain technologies for the Internet of Things:

Research issues and challenges," IEEE Internet Things J., vol. 6, no. 2, pp. 2188_2204, Apr. 2019.

[26] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, ``DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," IEEE Commun. Mag., vol. 55, no. 9, pp. 78_85, Sep. 2017.

[27] S. Rathore, B. W. Kwon, and J. H. Park, "Blockseciotnet: Blockchainbased decentralized security architecture for iot network," Journal of Network and Computer Applications, vol. 143, pp. 167–177, 2019.

[28] S. Boukria, M. Guerroumi, and I. Romdhani, "BCFR: Blockchain-based controller against false flow rule injection in SDN," in 2019 IEEE Symposium on Computers and Communications (ISCC). IEEE, 2019, pp. 1034–1039.

[29] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, "Blockchain-enabled authentication handover with efficient privacy protection in sdn-based 5g networks," IEEE Transactions on Network Science and Engineering, 2019.

[30] C. Qiu, F. R. Yu, H. Yao, C. Jiang, F. Xu, and C. Zhao, "Blockchainbased software-defined industrial internet of things: A dueling deep qlearning approach," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4627–4639, 2018.

[31] N. Oualha and K. T. Nguyen. Lightweight attribute-based encryption for the internet of things. In 2016 25th International Conference on Computer Communication and Networks (ICCCN), pages 1–6. IEEE, 2016.

[32] Y. Mao, J. Li, M.-R. Chen, J. Liu, C. Xie, and Y. Zhan. Fully secure fuzzy identity-based encryption for secure iot communications. Computer Standards & Interfaces, 44 :117–121, 2016.

[33] S. Tonyali, O. Cakmak, K. Akkaya, M. M. Mahmoud, and I. Guvenc. Secure data obfuscation scheme to enable privacy-preserving state estimation in smart grid ami networks. IEEE Internet of Things Journal, 3(5) :709–719, 2016.

[34] T. Hardjono and N. Smith. Cloud-based commissioning of constrained devices using permissioned blockchains. In Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security, pages 29– 36. ACM, 2016.

[35] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell. World of empowered iot users. In 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), pages 13–24. IEEE, April 2016.

[36] L. Kokoris-Kogias, L. Gasser, I. Khoffi, P. Jovanovic, N. Gailly, and B. Ford. Managing identities using blockchains and cosi. In 9th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2016), number EPFL-TALK-220210, 2016.

[37] K. Biswas and V. Muthukkumarasamy. Securing smart cities using blockchain technology. In 2016 IEEE 18th International Conference on High Performance Computing and communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pages 1392–1393. IEEE, Dec 2016.

[38] P. Bull, R. Austin, E. Popov, M. Sharma, and R. Watson. Flow based security for iot devices using an sdn gateway. In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Future Internet of Things and Cloud (FiCloud),, pages 157–163. IEEE, July 2016.

[39] C. Vandana. Security improvement in iot based on software defined networking (sdn). International Journal of Engineering and Technology Research (IJSETR), 5(1) :291–295, january 2016.

[40] C. Gonzalez, S. M. Charfadine, O. Flauzac, and F. Nolot. Sdnbased security framework for the iot in distributed grid. In 2016 International Multidisciplinary Conference on Computer and Energy Science (SpliTech), pages 1–5. IEEE, July 2016.

[41] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in International Conference on Advanced Communication Technology, 2017, pp. 464–467, doi: 10.23919/ICACT.2017.7890132.

[42] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the internet of things," Peer-to-Peer Networking and Applications, vol. 10, no. 4, pp. 983–994, Jul. 2017, doi: 10.1007/s12083-016-0456-1.

[43] H. F. Atlam, M. A. Azad, A. G. Alzahrani, and G. Wills, "A review of blockchain in internet of things and AI," Big Data and Cognitive Computing, vol. 4, no. 4, pp. 1–27, Oct. 2020, doi: 10.3390/bdcc4040028.

[44] M. A. Khan and K. Salah, "IoT security: review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, May 2018, doi: 10.1016/j.future.2017.11.022.

[45] S. Badr, I. Gomaa, and E. Abd-Elrahman, "Multi-tier blockchain framework for IoT-EHRs systems," Procedia Computer Science, vol. 141, pp. 159–166, 2018, doi: 10.1016/j.procs.2018.10.162.

[46] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in IoT: challenges and solutionss," Blockchain: Research and Applications, vol. 2, no. 2, 2021, doi: 10.1016/j.bcra.2021.100006.

[47] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: challenges and solutions," arxiv.org/abs/1608.05187, 2016, [Online]. Available: http://arxiv.org/abs/1608.05187.

[48] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: a state-of-the-art survey," IEEE Communications Surveys and Tutorials, vol. 21, no. 1, pp. 858–880, 2019, doi: 10.1109/COMST.2018.2863956.

[49] H. N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: a survey," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8076–8094, Oct. 2019, doi: 10.1109/JIOT.2019.2920987.

[50] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1594–1605, Apr. 2019, doi: 10.1109/JIOT.2018.2847705.

[51] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of IoT applications in blockchain systems," ACM Computing Surveys, vol. 53, no. 1, pp. 1–32, Jan. 2021, doi: 10.1145/3372136.

[52] A. S. Patil, B. A. Tama, Y. Park, and K. H. Rhee, "A framework for blockchain based secure smart green house farming," in Lecture Notes in Electrical Engineering, vol. 474, Springer Singapore, 2018, pp. 1162–1167.

[53] G. C. Polyzos and N. Fotiou, "Blockchain-assisted information distribution for the internet of things," in IEEE International Conference on Information Reuse and Integration (IRI), Aug. 2017, pp. 75–78, doi: 10.1109/IRI.2017.83.

[54] X. Zhu and Y. Badr, "Identity management systems for the internet of things: a survey towards blockchain solutions," Sensors, vol. 18, no. 12, Dec. 2018, doi: 10.3390/s18124215.

[55] S. Mishra and A. K. Tyagi, "Intrusion detection in internet of things (IoTs) based applications using blockchain technology," in Proceedings of the 3rd International Conference on I-SMAC IoT in Social, Mobile, Analytics and Cloud, Dec. 2019, pp. 123–128, doi: 10.1109/I-SMAC47947.2019.9032557.

[56] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet of things security: a position paper," Digital Communications and Networks, vol. 4, no. 3, pp. 149–160, Aug. 2018, doi: 10.1016/j.dcan.2017.10.006.

[57] X. Wang et al., "Survey on blockchain for internet of things," Computer Communications, vol. 136, pp. 10–29, Feb. 2019, doi: 10.1016/j.comcom.2019.01.006.

[58] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoTt," Journal of Network and Computer Applications, vol. 149, 2020, doi: 10.1016/j.jnca.2019.102481.

[59] E. F. Jesus, V. R. L. Chicarino, C. V. N. De Albuquerque, and A. A. D. A. Rocha, "A survey of how to use blockchain to secure internet of things and the stalker attack," Security and Communication Networks, vol. 2018, pp. 1–27, Apr. 2018, doi: 10.1155/2018/9675050.

[60] S. K. Dwivedi, P. Roy, C. Karda, S. Agrawal, and R. Amin, "Blockchain-based internet of things and industrial IoT: a comprehensive survey," Security and Communication Networks, vol. 2021, pp. 1–21, Aug. 2021, doi: 10.1155/2021/7142048.

[61] A. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldύ, "The rise of blockchain technology in agriculture and food supply chains," Trends in

Food Science and Technology, vol. 91, pp. 640–652, Sep. 2019, doi: 10.1016/j.tifs.2019.07.034.

[62] M. A. Ferrag, L. Maglaras, and H. Janicke, “Blockchain and its role in the internet of things,” in Springer Proceedings in Business and Economics, Springer International Publishing, 2019, pp. 1029–1038.

[63] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: architecture, consensus, and future trends,” in Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017, Jun. 2017, pp. 557–564, doi: 10.1109/BigDataCongress.2017.85.

[64] R. Thakore, R. Vaghashiya, C. Patel, and N. Doshi, “Blockchain - based IoT: a survey,” Procedia Computer Science, vol. 155, pp. 704–709, 2019, doi: 10.1016/j.procs.2019.08.101.

[65] F. Hassan et al., “Blockchain and the future of the internet: a comprehensive review,” arxiv.org/abs/1904.00733, Feb. 2019, [Online]. Available: http://arxiv.org/abs/1904.00733.

[66] J. Lin, Z. Shen, A. Zhang, and Y. Chai, “Blockchain and IoT based food traceability for smart agriculture,” in Proceedings of the 3rd International Conference on Crowd Science and Engineering, 2018, pp. 1–6, doi: 10.1145/3265689.3265692.

[67] E. M. Dogo, A. F. Salami, N. I. Nwulu, and C. O. Aigbavboa, “Blockchain and internet of things-based technologies for intelligent water management system,” in Artificial Intelligence in IoT, Springer International Publishing, 2019, pp. 129–150.

[68] S. B. Kadam and S. K. John, “Blockchain integration with low-power internet of things devices,” in Handbook of Research on Blockchain Technology, Elsevier, 2020, pp. 183–211.

[69] M. Maroufi, R. Abdolee, and B. M. Tazekand, “On the convergence of blockchain and internet of things (IoT) technologies,” Journal of Strategic Innovation and Sustainability, vol. 14, no. 1, Mar. 2019, doi: 10.33423/jsis.v14i1.990.

[70] M. Alamri, N. Z. Jhanjhi, and M. Humayun, “Blockchain for internet of things (IoT) research issues challenges & future directions: a review,” International Journalof Computer Science and Network Security, 2019.

[71] H. F. Atlam and G. B. Wills, “Intersections between IoT and distributed ledger,” in Advances in Computers, vol. 115, Elsevier, 2019, pp. 73–113.

[72] M. Saad et al., “Exploring the attack surface of blockchain: a systematic overview,” arxiv.org/abs/1904.03487, Apr. 2019, [Online]. Available: http://arxiv.org/abs/1904.03487.

[73] H. F. Atlam and G. B. Wills, “An efficient security risk estimation technique for risk-based access control model for IoT,” Internet of Things, vol. 6, Jun. 2019, doi: 10.1016/j.iot.2019.100052.

[74] A. Tandon, “An empirical analysis of using blockchain technology with internet of things and its application,” International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9S3, pp. 1469–1475, Aug. 2019, doi: 10.35940/ijitee.I3310.0789S319.

[75] P. Karthikeyyan, S. Velliangiri, and I. T. Joseph, “Review of blockchain based IoT application and its security issues,” in 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies, Jul. 2019, pp. 6–11, doi: 10.1109/ICICICT46008.2019.8993124.

[76] N. Fotiou, V. A. Siris, and G. C. Polyzos, “Interacting with the internet of things using smart contracts and blockchain technologies,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 11342, Springer International Publishing, 2018, pp. 443–452.

[77] L. Hang and D.-H. Kim, “Design and implementation of an integrated IoT blockchain platform for sensing data integrity,” Sensors, vol. 19, no. 10, May 2019, doi: 10.3390/s19102228.

[78] K. Mahmood et al., “PUF enable lightweight key-exchange and mutual authentication protocol for multi-server based D2D communication,” Journal of Information Security and Applications, vol. 61, Sep. 2021, doi: 10.1016/j.jisa.2021.102900.

[79] R. Alcarria, B. Bordel, T. Robles, D. Martín, and M.-Á. Manso-Callejo, ``A blockchain-based authorization system for trustworthy resource monitoring and trading in smart communities," Sensors, vol. 18, no. 10, p. 3561, Oct. 2018.

[80] A. G. Ghandour, M. Elhoseny, and A. E. Hassanien, ``Blockchains for smart cities: A survey," in Security in Smart Cities: Models, Applications, and Challenges. Springer, 2019, pp. 193_210.

[81] A. Rahman, M. K. Nasir, Z. Rahman, A. Mosavi, and B. Minaei-Bidgoli, ``DistBlockBuilding: A distributed blockchainbased SDN-IoT network for smart building management," IEEE Access, vol. 8, pp. 140008_140018, 2020.

[82] P. K. Sharma and J. H. Park, ``Blockchain based hybrid network architecture for the smart city," Future Gener. Comput. Syst., vol. 86, pp. 650_655, Sep. 2018.

[83] Y. Gu, D. Hou, X. Wu, J. Tao, and Y. Zhang, ``Decentralized transaction mechanism based on smart contract in distributed data storage," Information, vol. 9, no. 11, p. 286, Nov. 2018.

[84] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K.-R. Choo, ``An energy-ef_cient SDN controller architecture for IoT networks with blockchain-based security," IEEE Trans. Services Comput., vol. 13, no. 4, pp. 625_638, Jul. 2020.

[85] P. Singh, A. Nayyar, A. Kaur, and U. Ghosh, ``Blockchain and fog based architecture for Internet of everything in smart cities," Future Internet, vol. 12, no. 4, p. 61, Mar. 2020.

[86] P. K. Sharma, N. Kumar, and J. H. Park, ``Blockchain-based distributed framework for automotive industry in a smart city," IEEE Trans. Ind. Informat., vol. 15, no. 7, pp. 4197_4205, Jul. 2019.

[87] D. Sinh, L.-V. Le, B.-S. P. Lin, and L.-P. Tung, ``SDN/NFV_A new approach of deploying network infrastructure for IoT," in Proc. 27th Wireless Opt. Commun. Conf. (WOCC), Apr./May 2018, pp. 1_5.

[88] M. J. Islam, M. Mahin, S. Roy, B. C. Debnath, and A. Khatun, ``DistBlackNet: A distributed secure black SDN-IoT architecture with NFV implementation for smart cities," in Proc. Int. Conf. Electr., Comput. Commun. Eng. (ECCE), Feb. 2019, pp. 1_6.

[89] I. Abdulqadder, D. Zou, I. Aziz, B. Yuan, and W. Dai, ``Deployment of robust security scheme in SDN based 5G network over NFV enabled cloud environment," IEEE Trans. Emerg. Topics Comput., early access, Nov. 5, 2018.

[90] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, and K.-K.-R. Choo, ``BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system," Comput. Secur., vol. 85, pp. 288_299, Aug. 2019.

[91] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, ``DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," IEEE Commun. Mag., vol. 55, no. 9, pp. 78_85, Sep. 2017.

[92] B. K. Mukherjee, M. S. I. Pappu, M. J. Islam, and U. K. Acharjee, ``An SDN based distributed IoT network with NFV implementation for smart cities," in Proc. 2nd Int. Conf. Cyber Secur. Comput. Sci. (ICONCS). Springer, 2020, pp. 539_552.

[93] A. Rahman, U. Sara, D. Kundu, S. Islam, M. Jahidul, M. Hasan, Z. Rahman, and M. Kamal, ``DistB-SDoIndustry: Enhancing security in industry 4.0 services based on distributed blockchain through software de_ned networking-IoT enabled architecture," Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 9, 2020.

[94] A. Rahman, M. J. Islam, F. A. Sunny, and M. K. Nasir, ``DistblockSDN: A distributed secure blockchain based SDN-IoT architecture with NFV implementation for smart cities," in Proc. Int. Conf. Innov. Eng. Technol. (ICIET), 2019, pp. 23_24.

[95] Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of blockchains in the internet of things: A comprehensive survey. IEEE Commun. Surv. Tutor. 2018, 21, 1676–1717.

[96] Alladi, T.; Chamola, V.; Parizi, R.M.; Choo, K.-K.R. Blockchain applications for industry 4.0 and industrial IoT: A review. IEEE Access 2019, 7, 176935–176951.

[97] Xie, J.; Tang, H.; Huang, T.; Yu, F.R.; Xie, R.; Liu, J.; Liu, Y. A survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE Commun. Surv. Tutor. 2019, 21, 2794–2830.

[98] Yang, R.; Yu, F.R.; Si, P.; Yang, Z.; Zhang, Y. Integrated blockchain and edge computing systems: A survey, some research issues and challenges. IEEE Commun. Surv. Tutor. 2019, 21, 1508–1532.

[99] Ahmed, S.; Shah, M.A.; Wakil, K. Blockchain as a trust builder in the smart city domain: A systematic literature review. IEEE Access 2020, 8, 92977–92985.

[100] Ferrag, M.A.; Shu, L.; Yang, X.; Derhab, A.; Maglaras, L. Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. IEEE Access 2020, 8, 32031–32053.

[101] Wang, Q.; Zhu, X.; Ni, Y.; Gu, L.; Zhu, H. Blockchain for the IoT and industrial IoT: A review. Internet Things 2020, 10, 100081.

[102] Bhushan, B.; Sahoo, C.; Sinha, P.; Khamparia, A. Unification of blockchain and internet of things (BIoT): Requirements, working model, challenges and future directions. Wirel. Netw. 2021, 27, 55–90.

[103] Majeed, U.; Khan, L.U.; Yaqoob, I.; Kazmi, S.A.; Salah, K.; Hong, C.S. Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges. J. Netw. Comput. Appl. 2021, 181, 103007.

[104] Da Xu, L.; Lu, Y.; Li, L. Embedding blockchain technology into IoT for security: A survey. IEEE Internet Things J. 2021, 8, 10452–10473.

[105] Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. Neural Comput. Appl. 2022, 34, 11475–11490.

[106] Abdelmaboud, A.; Ahmed, A.I.A.; Abaker, M.; Eisa, T.A.E.; Albasheer, H.; Ghorashi, S.A.; Karim, F.K. Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. Electronics 2022, 11, 630.

[107] Kumar, R.L.; Khan, F.; Kadry, S.; Rho, S. A Survey on blockchain for industrial Internet of Things. Alex. Eng. J. 2022, 61, 6001–6022.

[108] Yu, Z.; Song, L.; Jiang, L.; Sharafi, O.K. Systematic literature review on the security challenges of blockchain in IoT-based smart cities. Kybernetes 2021, 51.

[109] Pennino, D.; Pizzonia, M.; Vitaletti, A.; Zecchini, M. Blockchain as IoT Economy enabler: A review of architectural aspects. J. Sens. Actuator Netw. 2022, 11, 20.

[110] Alkhateeb, A.; Catal, C.; Kar, G.; Mishra, A. Hybrid blockchain platforms for the internet of things (IoT): A systematic literature review. Sensors 2022, 22, 1304.