RESEARCH ARTICLE OPEN ACCESS

A Comprehensive Survey on Edge Computing Security: Challenges, Solutions, and Future Directions

Berthille Igiraneza

Computer Software, Nanjing University of Information Science and Technology, China

ABSTRACT

This survey paper provides an exhaustive examination of the security landscape within edge computing, identifying and dissecting the multifaceted security challenges that arise from its decentralized nature and widespread application across various domains such as Internet of Things (IoT), healthcare, smart cities, and autonomous driving. As edge computing pushes data processing to the edge of the network, closer to data sources, it introduces unique vulnerabilities and security concerns distinct from traditional cloud computing paradigms. This paper categorizes these security challenges into data security, network security, authentication, scalability, manageability, and privacy concerns. Through a systematic review, we evaluate a spectrum of existing security solutions, ranging from cryptographic methods and secure architectures to advanced authentication mechanisms and privacy-preserving techniques. Furthermore, the paper delves into emerging technologies like blockchain, artificial intelligence (AI), and quantum computing, exploring their potential to fortify security in edge computing environments. By highlighting current gaps, open issues, and potential future threats, this survey underscores the critical need for continued research, development of adaptive security strategies, and cross-disciplinary collaboration to navigate the evolving security landscape of edge computing. Through this comprehensive analysis, the paper aims to propel forward the discourse on edge computing security, paving the way for more secure, efficient, and reliable edge computing architectures.

Keywords :- Edge Computing Security, Cryptographic Methods, Privacy-preserving Techniques.

I. INTRODUCTION

In the ever-evolving landscape of digital technology, edge computing has emerged as a transformative force, ushering in a new era of data processing and analysis. By decentralizing computing resources and bringing them closer to the source of data—be it IoT devices, sensors, or smartphones—edge computing significantly reduces latency, minimizes bandwidth usage, and enhances overall system efficiency. This paradigm shift not only accelerates real-time data processing but also supports a myriad of applications, from autonomous vehicles and smart cities to healthcare monitoring systems, thereby playing a pivotal role in the modern digital ecosystem.

However, the distributed nature of edge computing introduces a complex array of security challenges. Traditional security models, often designed for centralized data processing environments, fall short in addressing the vulnerabilities inherent in the decentralized, heterogeneous, and highly dynamic edge environments. The proliferation of edge devices, each potentially becoming a new attack vector, underscores the importance of robust security measures. Moreover, the critical application areas of edge computing, many of which involve sensitive personal data or mission-critical operations, further amplify the need for comprehensive security solutions. The unique architecture of edge computing, combined with its broad application spectrum, thus demands a re-evaluation of conventional security strategies and the development of innovative solutions tailored to its specific needs.

The primary objective of this survey is to provide a thorough analysis of the current state of security within the realm of edge computing. This includes identifying the unique security challenges posed by edge computing architectures, reviewing existing solutions and technologies aimed at mitigating these risks, and exploring future directions for research and development in this domain. Through this paper, readers can expect to gain a comprehensive understanding of the security landscape of edge computing, including insights into the latest trends, potential vulnerabilities, and cutting-edge security measures.

The paper is structured as follows: Section 2 provides a background on edge computing, including its evolution, architecture, and key applications. Section 3 delves into the security challenges specific to edge computing, categorizing them into distinct areas for detailed analysis. Section 4 reviews existing security solutions, spanning from cryptographic methods to privacy-preserving techniques, and evaluates their applicability to edge computing. Section 5 explores emerging technologies and their potential impact on enhancing security in edge environments. In Section 6, we discuss current gaps, open issues, and anticipate future threats. Section 7 concludes the paper with a summary of findings and recommendations for future research directions. Through this structured approach, the paper aims to shed light on the pivotal role of security in enabling the safe and effective deployment of edge computing technologies.

II. BACKGROUND AND EVOLUTION OF EDGE COMPUTING

Edge computing refers to a distributed computing paradigm that brings computation and data storage closer to the location where it is needed, to improve response times and save bandwidth. Unlike traditional cloud computing, which relies on

centralized data centres far from the end-user, edge computing processes data near the source of data generation. This approach minimizes latency, reduces the load on the network, and enables real-time processing capabilities crucial for many modern applications [1, 2].

A. Historical Development

The concept of edge computing has evolved significantly over the past decade, driven by the exponential growth of IoT devices and the increasing demand for real-time computing. The term itself was coined in the early 2000s, but it gained significant traction in 2016 when the Edge Computing Consortium was established. Key milestones include the development of edge-specific technologies and standards, the introduction of edge computing platforms by major tech companies, and the integration of AI and machine learning algorithms into edge devices, enhancing their processing capabilities [3, 4].

B. Architecture

The architecture of edge computing is hierarchical and typically consists of three layers: the cloud, the edge, and the devices. The cloud layer houses centralized services and extensive computing resources. The edge layer includes edge servers and gateways located close to the data sources, which perform data processing and analytics. The device layer contains IoT devices and sensors that generate and initially process data. This architecture supports various functionalities, including data caching, local analytics, and decision-making processes, enabling faster response times and reduced bandwidth usage [5, 6].

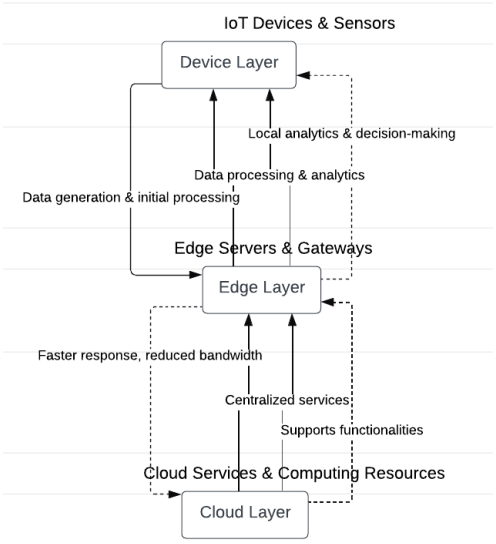

Fig. 1 Hierarchical architecture of edge computing

C. Application Areas

Edge computing has found applications across a wide range of sectors:

- IoT: In IoT, edge computing facilitates real-time data processing, enabling smart home devices, industrial automation, and energy management systems to function efficiently [7].
- Healthcare: Edge computing supports telemedicine, patient monitoring, and wearable health devices by providing immediate data analysis, which is crucial for life-saving decisions [8].
- Smart Cities: In smart cities, edge computing enables traffic management, public safety, and environmental monitoring through the immediate processing of data from various sensors and cameras [9].
- Autonomous Vehicles: For autonomous vehicles, edge computing provides the necessary real-time processing to support navigation, obstacle detection, and vehicle-to-vehicle communication [10].

I. III. SECURITY CHALLENGES IN EDGE COMPUTING

A. Data Security

In edge computing environments, data security is paramount due to the dispersed nature of data storage, transmission, and processing across the network edge. Edge devices generate substantial volumes of data, often processed locally, introducing risks such as data tampering, unauthorized access, and leakage [11]. The limited security capabilities of edge devices, compared to centralized data centres, exacerbate these vulnerabilities [12]. Furthermore, data in transit between edge devices and servers, or among edge devices themselves, faces risks of interception and eavesdropping, necessitating robust end-to-end encryption and integrity verification methods [13].

B. Network Security

Securing the communication channels within edge computing frameworks is critical to thwart attacks like man-in-the-middle, DoS, and spoofing. The reliance on wireless networks for such communications introduces additional vulnerabilities targeted by adversaries [14]. Implementing comprehensive security protocols to protect data in transit in these resource-constrained environments is challenging yet essential [15]. The network's dynamic topology, with devices frequently joining and leaving, further complicates network security management.

C. Authentication and Access Control

Ensuring that only authorized entities can access edge computing resources is crucial. The diversity of devices, each with varying capabilities and security levels, poses significant challenges in deploying uniform authentication and access control mechanisms [16]. Traditional authentication methods may not suit the limited power and computational resources of many edge devices. This scenario calls for lightweight, secure authentication protocols tailored for rapid processing needs [17, 18].

D. Scalability and Manageability

The management and scalability of security policies across the multitude of devices in edge computing are hindered by their diversity in hardware and software configurations. Automating the security policy deployment and updates across such a vast, dynamic environment remains a formidable challenge [19]. Security solutions must be scalable and adaptable, without overwhelming the computational capabilities of edge devices [20].

E. Privacy

Privacy in edge computing is a critical concern, especially as devices in various environments collect sensitive personal information. The risk of privacy breaches increases in distributed processing settings, where data may traverse multiple potentially vulnerable nodes [21]. Implementing privacy-preserving techniques like data anonymization in such settings is complex, yet crucial for maintaining user privacy and compliance with regulations like GDPR [22].

TABLE I EDGE COMPUTING SECURITY CHALLENGES SUMMARY

Security Challenge	Description
Data Security	Concerns related to data storage, transmission, and processing at the edge.
Network Security	Challenges in securing the communication between edge devices and central servers or between edge devices themselves.
Authentication and Access Control	Issues in ensuring that only authorized devices and users can access and execute computing tasks.
Scalability and Manageability	The difficulty of maintaining security policies across numerous and often heterogeneous devices.
Privacy	Ensuring user privacy when personal data is processed closer to its source.

II. IV. REVIEW OF EXISTING SECURITY SOLUTIONS

A. Cryptographic Techniques

Cryptographic techniques are fundamental to securing data within edge computing environments, both at rest and in transit. Encryption algorithms, such as Advanced Encryption Standard (AES) and public-key infrastructures (PKIs), provide the means to securely encrypt data, ensuring that even if data is intercepted, it remains unintelligible to unauthorized parties. Hash functions and digital signatures further ensure data integrity and non-repudiation, crucial for maintaining trust in distributed systems. Symmetric key algorithms offer efficiency for resource-constrained devices, while asymmetric cryptography facilitates secure key exchange over unsecured channels [23, 24].

B. Secure Architectures

Developing secure architectures involves creating designs and frameworks that inherently incorporate security as a core aspect of edge computing environments. This includes deploying security services directly on edge devices or through edge servers, integrating intrusion detection systems (IDS), and employing security information and event management (SIEM) systems tailored for edge environments. Such architectures often leverage virtualization and containerization to isolate sensitive computations and data, minimizing the attack surface. Software-Defined Networking (SDN) and Network Function Virtualization (NFV) also play roles in dynamically managing network security policies and resources.

C. Authentication Mechanisms

Authentication mechanisms in edge computing ensure that only authorized devices and users can access resources. Traditional approaches like username/password are increasingly supplemented or replaced by more secure and convenient methods. Biometric authentication leverages unique physical characteristics, offering a high level of security and ease of use. Blockchain technology, with its decentralized nature, provides a robust framework for secure, tamper-proof authentication and access control, ensuring device and user authenticity across distributed networks [25, 26].

D. Privacy-preserving Solutions

Preserving privacy in edge computing, especially when processing personal data, is critical. Federated learning, a machine learning approach, allows edge devices to collaboratively learn a shared model while keeping all the training data on device, thus not exposing it to central servers or potential adversaries. Differential privacy introduces noise to datasets or query results, making it difficult to infer individual data points while still allowing for accurate aggregate analysis. These techniques ensure that user data is protected and that privacy regulations are complied with [27, 28].

E. Case Studies

Real-world applications of these security solutions highlight their practical value and effectiveness. For instance, in smart healthcare systems, cryptographic techniques secure patient data transmitted from wearable devices to healthcare providers. Secure architectures with embedded IDS have been deployed in smart grid systems to detect and mitigate threats in real-time. Blockchain-based authentication mechanisms are increasingly used in supply chain management to verify the authenticity of products and participants. In smart city projects, federated learning and differential privacy techniques are applied to traffic and pollution monitoring data to optimize city management without compromising the privacy of citizens [29, 30].

III. V. EMERGING TECHNOLOGIES AND FUTURE DIRECTIONS

A. Blockchain

Blockchain technology stands at the forefront of revolutionizing security in edge computing through its inherent characteristics of decentralization, transparency, and immutability. It offers a robust solution for secure, decentralized integrity verification and management of transactions and interactions between edge devices. By leveraging blockchain, edge computing networks can establish trust among devices, manage identities securely, and ensure data integrity without relying on centralized authorities. This technology is particularly promising for applications requiring stringent security measures, such as smart contracts in supply chains or identity verification in smart cities, where the integrity and non-repudiation of transactions are critical [31, 32].

B. Artificial Intelligence and Machine Learning

Artificial Intelligence (AI) and Machine Learning (ML) technologies are increasingly being integrated into edge computing to enhance security through predictive analytics, anomaly detection, and automated threat responses. Machine learning models can analyze patterns from vast amounts of data generated at the edge to identify potential security threats in real-time. AI algorithms can then automate responses to these threats, enhancing the resilience of edge networks. Moreover, AI-driven security systems can adapt to evolving threats over time, learning from new data and attacks to continuously improve their defense mechanisms. This adaptive security approach is crucial in the dynamically changing environments of edge computing [33].

C. Quantum Computing

The advent of quantum computing presents both opportunities and challenges for the security of edge computing. On one hand, quantum computing threatens to break current cryptographic protocols by solving problems that are infeasible for classical computers, such as factoring large primes used in RSA encryption. On the other hand, it also offers the potential for quantum-resistant cryptographic algorithms and quantum key distribution (QKD), which could provide unprecedented levels of security. As such, the edge computing community must anticipate the impact of quantum computing on security paradigms and begin integrating quantum-resistant cryptographic methods to safeguard future communications and data [34].

D. Regulatory and Standardization Efforts

The role of regulations and standardization is becoming increasingly crucial in shaping security practices within edge computing. Regulatory frameworks, such as the General Data Protection Regulation (GDPR) in the European Union, set stringent requirements for data privacy and security, driving the need for compliant security solutions in edge computing environments. Similarly, standardization bodies, such as the Institute of Electrical and Electronics Engineers (IEEE) and the International Organization for Standardization (ISO), are working to establish security standards specific to edge computing. These efforts aim to harmonize security practices across the industry, providing clear guidelines for the development, deployment, and evaluation of secure edge computing solutions. Standardization not only facilitates interoperability among diverse edge devices but also ensures that security considerations are uniformly addressed across different platforms and applications [35, 36].

IV. VI. CHALLENGES AND OPEN ISSUES

A. Technical Limitations

Despite significant advancements, edge computing faces technical limitations that hinder the deployment of effective security measures. These limitations include constrained computational resources, limited battery life of edge devices, and the inherent complexity of managing a vast network of distributed nodes. Such constraints make it challenging to implement sophisticated security algorithms that require substantial computational power and energy. Moreover, the vast and varied nature of edge devices introduces complexities in deploying uniform security protocols, making some devices more vulnerable to attacks than others.

B. Adaptability

The dynamic nature of edge computing, characterized by constantly evolving architectures and threat landscapes, demands highly adaptable security solutions. Traditional security mechanisms, designed for static networks, struggle to cope with the fluidity of edge environments. Security solutions must, therefore, be capable of automatically adapting to changes in network topology, device configurations, and emerging threats. This adaptability is crucial for maintaining the integrity and confidentiality of data as new types of devices are added and as the applications of edge computing expand into new domains.

C. Interoperability

Interoperability remains a significant challenge in edge computing, given the diversity of devices, manufacturers, and protocols within the ecosystem. Ensuring compatibility among these diverse components is essential for seamless operation and for implementing end-to-end security measures. The lack of standardized protocols exacerbates this challenge, leading to potential security gaps where interoperability is forced through ad-hoc solutions. Efforts toward standardization and the development of universal security protocols are necessary to address these interoperability challenges and to ensure that security measures are comprehensive and uniformly applied across all devices and layers of the network.

D. Future Threats

As edge computing technologies advance, they will inevitably face new types of security threats. These future threats may exploit vulnerabilities unique to edge computing architectures, such as the decentralized nature of data processing or the use of predictive analytics. For instance, AI and ML models deployed at the edge for security purposes themselves may become targets, with attackers using

adversarial techniques to manipulate these models. Anticipating and mitigating such threats require ongoing research and development efforts focused on understanding potential vulnerabilities and on designing security measures that can evolve in response to new types of attacks.

VII. CONCLUSION

A. Summary

The exploration of security in edge computing reveals a landscape rich with potential yet fraught with challenges. At its core, edge computing represents a paradigm shift towards decentralized data processing, bringing computation closer to data sources and thereby enhancing efficiency and reducing latency. However, this shift introduces unique security vulnerabilities that traditional, centralized models of security are ill-equipped to address. From data security and network protection to authentication and privacy concerns, the security challenges in edge computing are as diverse as they are critical. The review of existing security solutions, including cryptographic techniques, secure architectures, and privacy-preserving methods, underscores the concerted effort by the research community to fortify edge computing environments against malicious actors.

B. Insights Gained

This survey has illuminated several key findings: First, the implementation of blockchain and AI/ML technologies in edge computing offers promising avenues for enhancing security, from decentralized integrity verification to predictive threat detection and response. Second, the adaptability and scalability of security solutions are paramount, given the dynamic and heterogeneous nature of edge computing architectures and the evolving landscape of cyber threats. Third, interoperability emerges as a significant hurdle, emphasizing the need for standardized security protocols across diverse devices and platforms. Lastly, the imminent advent of quantum computing poses both a threat to current cryptographic methods and an opportunity for developing quantum-resistant algorithms, signalling a forthcoming pivotal shift in cybersecurity paradigms.

C. Call to Action

The complex security landscape of edge computing necessitates ongoing research and innovation to identify and mitigate emerging threats. This calls for a collaborative approach that transcends disciplinary boundaries, bringing together academia, industry, and regulatory bodies. Academia must continue to advance our understanding of edge computing security through research and development, while industry players should prioritize the implementation of secure technologies and practices in their products and services. Regulatory bodies, on the other hand, play a crucial role in establishing clear security standards and frameworks that guide and govern the deployment of edge computing technologies. Together, these efforts will ensure the secure and trustworthy evolution of edge computing, enabling it to reach its full potential in driving forward our increasingly connected world.

In conclusion, while the journey to securing edge computing is fraught with challenges, it also presents an opportunity for innovation, collaboration, and progress. By addressing the highlighted security challenges head-on, the global community can unlock the transformative potential of edge computing, paving the way for a more efficient, responsive, and secure digital future.

REFERENCES

[1] M. Satyanarayanan, "The Emergence of Edge Computing," *Computer*, vol.50(1), pp. 30-39, 2017.

[2] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu. "Edge Computing: Vision and Challenges," IEEE *Internet of Things Journal*, vol.3(5), pp. 637-646, 2016.

[3] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher and V. Young, "Mobile Edge Computing—A Key Technology Towards 5G," *ETSI White Paper*, No. 11, 2015.

[4] G. Premsankar, M. Di Francesco and T. Taleb, "Edge Computing for the Internet of Things: A Case Study," *IEEE Internet of Things Journal*, vol. 5(2), pp. 1275-1284, 2018.

[5] B. Varghese, N. Wang, S. Barbhuiya, P. Kilpatrick and D. S. Nikolopoulos, "Challenges and Opportunities in Edge Computing," *IEEE International Conference on Smart Cloud (SmartCloud)*, pp. 20-26, 2016.

[6] W. Shi, X. Zhang andY. Zhong, "Edge Computing: State-of-the-Art and Future Directions," *Journal of Computer Research and Development*, vol. 57(1), pp. 1-33, 2020.

[7] H. Gupta, A. Vahid Dastjerdi, S. K. Ghosh and R. Buyya, "iFogSim: A Toolkit for Modeling and Simulation of Resource Management Techniques in the Internet of Things, Edge and Fog Computing Environments," *Software: Practice and Experience*, vol. 47(9), pp. 1275-1296, 2017.

[8] A. M. Rahmani, T. N. Gia, B. Negash, A. Anzanpour, I. Azimi, M. Jiang and P. Liljeberg, "Exploiting Smart E-Health Gateways at the Edge of Healthcare Internet-of-Things: A Fog Computing Approach," *Future Generation Computer Systems*, vol. 78, pp. 641-658, 2018.

[9] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet of Things Journal*, vol. 1(1), pp. 22-32, 2014.

[10] M. Gerla, E. K. Lee, G. Pau andU. Lee, "Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds," *IEEE World Forum on Internet of Things (WF-IoT)*, pp. 241-246, 2014.

[11] L. U. Khan and K. Salah, "IoT Security: Review, Blockchain Solutions, and Open Challenges," *Future Generation Computer Systems*, vol. 82, pp. 395-411, 2018.

[12] R. Roman, J. Lopez and M. Mambo, "Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges," *Future Generation Computer Systems*, vol. 78, pp. 680-698, 2018.

[13] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin and X. Yang, "A Survey on the Edge Computing for the

Internet of Things," *IEEE Access*, vol. 6, pp. 6900-6919, 2020.

[14] A. Alrawais, A. Alhothaily, C. Hu and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," *IEEE Internet Computing*, vol. 21, no. (2), pp. 34-42, 2017.

[15] A. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, S. Choudhury and V. Kumar, "Security and Privacy in Fog Computing: Challenges," *IEEE Access*, vol. 6, pp. 18209-18237, 2018.

[16] J. Dizdarevic, F. Carpio, A. Jukan and X. Masip-Bruin, "Survey on IoT Solutions Aimed at IoT Connectivity, Device, and Thing's Management," *IEEE Access*, vol. 7, pp. 58830-58853, 2019.

[17] N. Fernando, S. W. Loke and W. Rahayu, "Mobile Edge Computing: A Survey," *Future Generation Computer Systems*, vol. 87, pp. 890-902, 2018.

[18] A. Ouaddah, A. Abou Elkalam and A. Ait Ouahman, "FairAccess: A New Blockchain-Based Access Control Framework for the Internet of Things," *Security and Communication Networks*, 2017.

[19] J. Ni, K. Zhang, X. Lin and X. Shen, "Securing Fog Computing for Internet of Things Applications: Challenges and Solutions," *IEEE Communications Surveys & Tutorials*, vol. 20(1), pp. 601-628, 2018.

[20] D. He, S. Chan and M. Guizani, "Secure and Lightweight Network Admission and Transmission Protocol for Body Sensor Networks," *IEEE Journal of Biomedical and Health Informatics*, vol. 22(6), pp. 1838-1847, 2018.

[21] P. Gope ad B. Sikdar, "Lightweight and Privacy-Preserving Secure Data Aggregation Scheme for Fog Computing-Enhanced IoT," *IEEE Access*, vol. 8, pp. 19345-19357, 2020.

[22] S. Li, L. Da Xu and S. Zhao, "5G Internet of Things: A Survey," *Journal of Industrial Information Integration*, vol. 10, pp. 1-9, 2018.

[23] F. A. Alaba, M. Othman, I. A. T. Hashem and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10-28, 2017.

[24] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren and X.S. Shen, 'Security and privacy in smart city applications: Challenges and solutions,' *IEEE Communications Magazine*, vol.55(1), pp. 122-129.

[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 of Things Journal*, vol. 6(2), pp. 2188-2204, 2018.

[26] M.B. Mollah, J. Zhao, D. Niyato and L.H. Koh, "Blockchain for the Internet of Vehicles towards intelligent transportations systems: A survey," *IEEE Internet of Things Journal*, vol.8(6), pp. 4157-4185, 2020.

[27] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao and S. Liu, "Applications of federated learning in smart cities: Recent advances and future directions," *IEEE Access*, vol. 8, pp. 153803-153815, 2018.

[28] Q. Yang, Y. Liu, T. Chen and Y. Tong, "Federated machine learning: Concept and applications." *ACM Transactions on Intelligent Systems and Technology*, vol.10(2), pp. 1-19, 2019.

[29] K. Shafique, A. B. Khawaja, F. Sabir, S. Qazi and M. Mustaqim, "An efficient data security model for fog computing," *IEEE Access*, vol. 8, pp. 91045-91056, 2020.

[30] S. Wang, Y. Zhang, L. Wang and B. Yang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol.7, pp. 38437-38450, 2019.

[31] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol.4, pp. 2292-2303, 2016.

[32] A. Reyna, C. Martin, J. Chen, E. Soler and M. Diaz, "On blockchain and Its Integration with IoT. Challenges and Opportunities," *Future Generation Computer Systems*, vol.88, pp. 173-190, 2018.

[33] D. Li, D. Chen, J. Wan, X. Li, C. Liu and S. Wang, "Artificial Intelligence with Multi-functional Machine Learning Platform Development for Better Healthcare and Precision Medicine," Database, 2020.

[34] M. Mosca, M. Roetteler and T. Takagi, "Quantum Computing for everyone," MIT press, 2019.

[35] R. Roman, J. Zhou and J. Lopez, "On the features and Challenges of Security and Privacy in Distributed Internet of Things," *Computer Networks*, vol. 57(10), pp. 2266-2279, 2018.

[36] R. H. Weber, "Internet of Things-New security and privacy challenges," *Computer Law & Security Review*, vol. 26(1), pp. 23-30, 2010.