A Secure Block chain-Based Scheme for IOT Data Credibility in Fog Environment

Saikumar Shetti[1], Mothith Pandey[2], Rohith Nagapuri[3], S.Sandhya[4]

[1,2,3]Scholar, Department of CSE in Jayamukhi institute of technological sciences, Narsampet, Warangal, Telangana, India

[4]Assistant professor, Department of CSE in Jayamukhi institute of technological sciences, Narsampet, Warangal, Telangana, India

ABSTRACT

The reliability of data is an essential component in the process of making decisions in businesses and governments that are supported by facts (e.g., policy making). Within a fog environment, the devices and systems that are connected to the Internet of Things (IoT) are an example of one of the most important data sources. However, the increasing complexity and interconnectivity of environments like the Internet of Things and fog can result in security vulnerabilities (for example, as a result of implementation errors or flaws in the underlying devices or systems). These vulnerabilities can be manipulated to make concessions the credibility of the data. As a result, in this paper, we present a safe Cryptocurrency scheme to guarantee the reliability of node or data and assure the security of data transmission in an environment that is characterised by fog. Experimentation are then used to show that the suggested plan is practical.

I INTRODUCTION

The process of making judgments in organisations and governments that are backed by facts requires an important component, and that component is the dependability of the data (e.g., policy making). The devices and systems that are linked to the Internet of Things (IoT) are an example of one of the most significant data sources that can be found inside an environment that utilises fog computing. On the other hand, the Internet of Things and fog settings are becoming more complicated and interconnected, which might lead to security risks (for example, as a result of implementation errors or flaws in the underlying devices or systems). These weaknesses are susceptible to manipulation, which may result in compromises made to the data's trustworthiness. As a consequence of this, in this work, we provide a risk-free Cryptocurrency system to ensure the dependability of nodes or data and to insure the security of data transmission in an environment that is characterised by fog. The results of the experiments are then utilised to demonstrate that the proposed strategy is feasible. a comparison of the two ideas highlighting their contrasts. [1]. The former (fog computing) may be thought of as a platform that is highly virtualized between the cloud data centre and terminal installations. This platform gives users the capacity to compute, store, and provide online services [2]. In general, a fog environment consists of key fog nodes that are connected to a variety of Internet of Things devices located in various localised regions or areas, and these nodes are tasked with the responsibility of temporarily storing data that is collected in the Internet of Things devices to which they are connected (e.g., sensors). The latter will, in general, sense, collect, and transmit the information to the fog nodes for the purpose of preprocessing, preliminary analysis, and/or forwarded to the cloud server for further data analytics; this will support more innovative and complex truly big data analysis (for example, data collected from various fog environments). In addition to this, fog environments boost the effectiveness of communication and provide enhanced support for real-time applications (for example, real-time data interchange and decision making in the context of Internet of Vehicles settings and healthcare/wellbeing contexts) [3]–[6].

There is no such thing as a flawless system, and similarly, there are a variety of obstacles that come with fog-filled settings. For instance, how can we efficiently and effectively authenticate the fog nodes, taking into account their diversity (hardware/software, located at different control layers, etc.) [7], and/or detect (potentially) malicious data that are in transit between different fog environments [8], [28], for instance, as a result of man-in-the-middle and other attacks [9]? [7] [8] [28] [9] [8] [28] [8] [28] [Also, how can we protect the privacy of the user without compromising the system's overall performance and safety [10, 29]?

These challenges highlight how important it is to design an approach that is both dynamic and secure, as well as sufficiently robust to work in the varied environments of fog computing, such as the requirements and limitations of hardware and software, the network, and the physical settings, among other factors. In the research that has been done, many methods have been suggested. For instance, Law et al. [17] established a key management platform that they called WAMS in order to accomplish the security goals for communications. Balfanz et al. [18] suggested a safe, user-friendly, and economical way for achieving authentication in local ad hoc wireless networks. In this system, the preauthentication is accomplished via physical touch in a location-constrained channel. A strategy was developed by Han et al. [19] to identify rogue access points in fog settings. More specifically, the technique makes advantage of the round-trip time between DNS servers and end users to ease the identification of rogue access points.

Mobile online social networks rely heavily on users' ability to share their whereabouts (and many other networks and services). Massive amounts of sensitive user information are gathered, distributed, analysed, and stored in order to make it possible for users to share their whereabouts in an accurate and efficient manner.

There are obvious issues about privacy, which is why Wei et al. [20] established a framework for location sharing that protects users' privacy and is designed for use in mobile online social networks. In order to improve data exchange in fog and cloud settings, Yu et al. [21] offered a method that would provide scalable, confidential, and fine-grained access control. This would be especially helpful in situations where untrusted third-party organisations were involved. A method was presented by Cao et al. [22] to increase the data dependability in fog situations. More specifically, they focused on data mending and corruption detection without requiring a significant amount of processing effort. Damiani et al. [23] developed a reliable reputation sharing technique that is based on accessible Peer-to-Peer (P2P) protocols. Within this mechanism, an autonomously self-regulating network architecture is implemented in order to safeguard the anonymity of data consumers.

A fresh framework for a mobile cloud computing environment was proposed by Shi et al. [24]. [Citation needed] A network trust shielding for mobile devices is included in their design. This shielding is especially effective against malware and illegal access. Nevertheless, it is possible that the solutions that are now available may be inadequate against newer or developing security assaults in fog settings, especially as the quantity of data that has to be analysed rises. Additionally, it's possible that present methods may not offer a solution that protects users' privacy and is lightweight.

In the interest of making a contribution to the current body of research, we provide a secure Blockchain-based scheme (SBBS) that is intended to verify the reliability of source data in situations characterised by fog. To be more specific, SBBS assists us in ensuring that data remain unchanged throughout the handling and transmission process as well as locating rogue nodes. To guarantee that our method is lightweight, we make use of an attribute-based signature, often known as an ABS.

II EXISTING SYSTEM

The process of making judgments in companies and agencies that are backed by facts requires an important component, and

that component is the dependability of the data (e.g., policy making). The equipments that are linked to the Internet of Things (IoT) are an illustration and one of the most significant data sources that can be found inside an atmosphere that utilises fog computing. On the other hand, the Internet of Things and fog settings are becoming more complicated and interconnected, which might lead to security risks (for example, as a result of implementation errors or flaws in the underlying devices or systems). These weaknesses are susceptible to manipulation, which may result in compromises made to the data's trustworthiness. As a consequence of this, in this work, we provide a risk-free Cryptocurrency system to ensure the dependability of nodes or data and to insure the protection of information transportation in an environments characterized by fog. The results of the experiments are then utilised to demonstrate that the proposed strategy is feasible. a comparison of the two ideas highlighting their contrasts. [1]. The former (fog computing) may be thought of as a platform that is highly virtualized between the cloud data centre and endpoint deployments. This platform gives users the capacity to compute, store, and provide online services [2]. In general, a fog environment consists of key fog nodes that are connected to a variety of Internet of Things devices located in various localised regions or areas, and these nodes are tasked with the responsibility of capturing and storing data which was collected in the Internet of Things devices to which they are connected (e.g., sensors). The latter will, in general, sense, collect, and transmit the information to the fog nodes for the purpose of preprocessing, preliminary analysis, and/or forwarded to the cloud server for further data analytics; this will encourage more groundbreaking and complex truly big data analysis (for example, data collected from various fog environments). In addition to this, fog environments boost the effectiveness of communication and provide enhanced support for real-time applications (for example, real-time data interchange and decision - making process in the context of Internet of Vehicles settings and healthcare/wellbeing contexts) [3]–[6].

There is no such thing as a flawless system, and similarly, there are a variety of obstacles that come with fog-filled settings. For instance, how can we efficiently and effectively authenticate the fog nodes, taking into account their diversity (hardware/software, located at different control layers, etc.) [7], and/or detect (potentially) malicious data that are already in transit between different fog surroundings [8], [28], for instance, as a result of man-in-the-middle and also other attacks [9]? [7] [8] [28] [9] [8] [28] [8] [28] [Also, how can we protect the privacy of the user without compromising the efficiency of the process and safety [10, 29]?

These challenges highlight how important it is to design an approach that is both dynamic and secure, as well as sufficiently robust to work in the varied environments of fog computing, such as the requirements and specifications of hardware and software, the network, and the physical settings, among other factors. In the research that has been done, many methods have been suggested.

For instance, Law et al. [17] established a key management platform that they called WAMS in order to accomplish the security goals for communications. Balfanz et al. [18] suggested a safe, user-friendly, and economical way for achieving authentication in local ad hoc wireless networks. In this system, the preauthentication is accomplished via physical touch in a location-constrained channel. A strategy was developed by Han et al. [19] to identify rogue access points in fog settings. More specifically, the technique makes advantage of the round-trip time between DNS servers and end users to ease the identification of rogue access points.

Mobile online social networks rely heavily on users' ability to share their whereabouts (and many other networks and services). Massive amounts of sensitive user information are gathered, distributed, analysed, and stored in order to make it possible for users to share

their whereabouts in an accurate and efficient manner.

There are obvious issues about privacy, which is why Wei et al. [20] established a framework for location sharing that protects users' privacy and is designed for use in mobile online social networks. In order to improve data exchange in fog and cloud settings, Yu et al. [21] offered a method that would provide scalable, confidential, and fine-grained access control. This would be especially helpful in situations where untrusted third-party organisations were involved. A method was presented by Cao et al. [22] to increase the data dependability in fog situations. More specifically, they focused on data mending and corruption detection without requiring a significant amount of processing effort. Damiani et al. [23] developed a reliable reputation sharing technique that is based on accessible Peer-to-Peer (P2P) protocols. Within this mechanism, an autonomously self-regulating network architecture is implemented in order to safeguard the anonymity of data consumers.

A fresh framework for a cloud setup was proposed by Shi et al. [24]. [Citation needed] A network trust shielding for mobile devices is included in their design. This shielding is especially effective against malware and illegal access. Nevertheless, it is possible that the solutions that are now available may be inadequate against newer or developing security assaults in fog settings, especially as the quantity of data that has to be analysed rises. Additionally, it's possible that present methods may not offer a solution that protects users' privacy and is lightweight.

In the interest of making a contribution to the current body of research, we provide a secure Blockchain-based scheme (SBBS) that is intended to verify the reliability of source data in situations characterised by fog. To be more specific, SBBS assists us in ensuring that data remain unchanged throughout the handling and transmission process as well as locating rogue nodes. To guarantee that our method is lightweight, we make use of an attribute-based signature, often known as an ABS.

III PROPOSED SYSTEM

The process of making judgments in companies and agencies that are backed by facts requires an important component, and that component is the dependability of the data (e.g., policy making). The equipments that are linked to the Internet of Things (IoT) are an illustration and one of the most significant data sources that can be found inside an atmosphere that utilises fog computing. On the other hand, the Internet of Things and fog settings are becoming more complicated and interconnected, which might lead to security risks (for example, as a result of implementation errors or flaws in the underlying devices or systems). These weaknesses are susceptible to manipulation, which may result in compromises made to the data's trustworthiness. As a consequence of this, in this work, we provide a risk-free Cryptocurrency system to ensure the dependability of nodes or data and to insure the protection of information transportation in an environments characterized by fog.

The results of the experiments are then utilised to demonstrate that the proposed strategy is feasible. a comparison of the two ideas highlighting their contrasts. [1]. The former (fog computing) may be thought of as a platform that is highly virtualized between the cloud data centre and endpoint deployments. This platform gives users the capacity to compute, store, and provide online services [2]. In general, a fog environment consists of key fog nodes that are connected to a variety of Internet of Things devices located in various localised regions or areas, and these nodes are tasked with the responsibility of capturing and storing data which was collected in the Internet of Things devices to which they are connected (e.g., sensors).

The latter will, in general, sense, collect, and transmit the information to the fog nodes for the purpose of preprocessing, preliminary analysis, and/or forwarded to the cloud server for further data analytics; this will encourage more groundbreaking and complex truly big data analysis (for example, data collected from various fog environments). In addition to this,

fog environments boost the effectiveness of communication and provide enhanced support for real-time applications (for example, real-time data interchange and decision - making process in the context of Internet of Vehicles settings and healthcare/wellbeing contexts) [3]–[6].

There is no such thing as a flawless system, and similarly, there are a variety of obstacles that come with fog-filled settings. For instance, how can we efficiently and effectively authenticate the fog nodes, taking into account their diversity (hardware/software, located at different control layers, etc.) [7], and/or detect (potentially) malicious data that are already in transit between different fog surroundings [8], [28], for instance, as a result of man-in-the-middle and also other attacks [9]? [7] [8] [28] [9] [8] [28] [8] [28] [Also, how can we protect the privacy of the user without compromising the efficiency of the process and safety [10, 29]?

These challenges highlight how important it is to design an approach that is both dynamic and secure, as well as sufficiently robust to work in the varied environments of fog computing, such as the requirements and specifications of hardware and software, the network, and the physical settings, among other factors. In the research that has been done, many methods have been suggested. For instance, Law et al. [17] established a key management platform that they called WAMS in order to accomplish the security goals for communications. Balfanz et al. [18] suggested a safe, user-friendly, and economical way for achieving authentication in local ad hoc wireless networks. In this system, the preauthentication is accomplished via physical touch in a location-constrained channel. A strategy was developed by Han et al. [19] to identify rogue access points in fog settings. More specifically, the technique makes advantage of the round-trip time between DNS servers and end users to ease the identification of rogue access points.

Mobile online social networks rely heavily on users' ability to share their whereabouts (and many other networks and services). Massive amounts of sensitive user information are gathered, distributed, analysed, and stored in order to make it possible for users to share their whereabouts in an accurate and efficient manner.

There are obvious issues about privacy, which is why Wei et al. [20] established a framework for location sharing that protects users' privacy and is designed for use in mobile online social networks. In order to improve data exchange in fog and cloud settings, Yu et al. [21] offered a method that would provide scalable, confidential, and fine-grained access control. This would be especially helpful in situations where untrusted third-party organisations were involved. A method was presented by Cao et al. [22] to increase the data dependability in fog situations. More specifically, they focused on data mending and corruption detection without requiring a significant amount of processing effort.

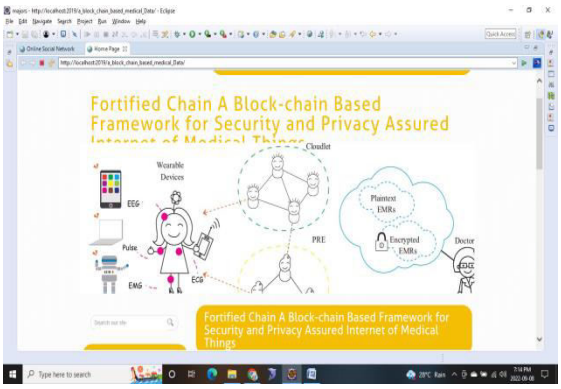
Damiani et al. [23] developed a reliable reputation sharing technique that is based on accessible Peer-to-Peer (P2P) protocols. Within this mechanism, an autonomously self-regulating network architecture is implemented in order to safeguard the anonymity of data consumers.

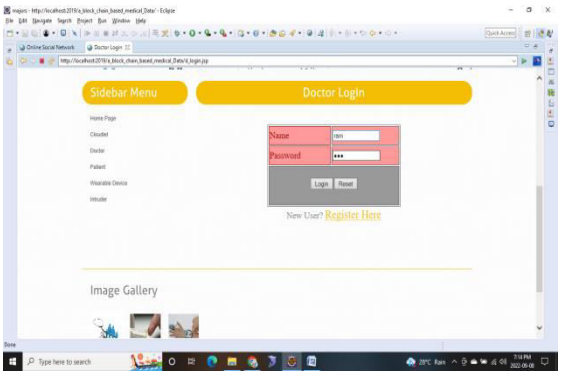
A fresh framework for a cloud setup was proposed by Shi et al. [24]. [Citation needed] A network trust shielding for mobile devices is included in their design. This shielding is especially effective against malware and illegal access. Nevertheless, it is possible that the solutions that are now available may be inadequate against newer or developing security assaults in fog settings, especially as the quantity of data that has to be analysed rises. Additionally, it's possible that present methods may not offer a solution that protects users' privacy and is lightweight.

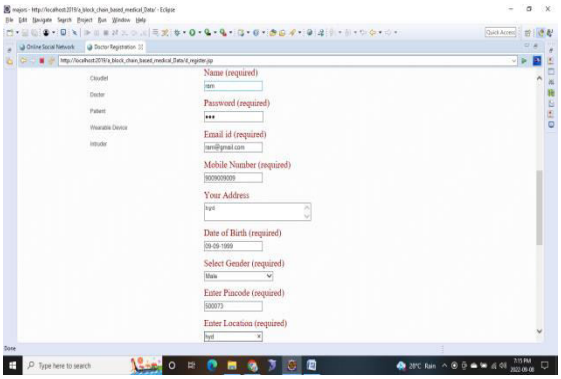
In the interest of making a contribution to the current body of research, we provide a secure Blockchain-based scheme (SBBS) that is intended to verify the reliability of source data in situations characterised by fog. To be more specific, SBBS assists us in ensuring that data remain unchanged throughout the handling

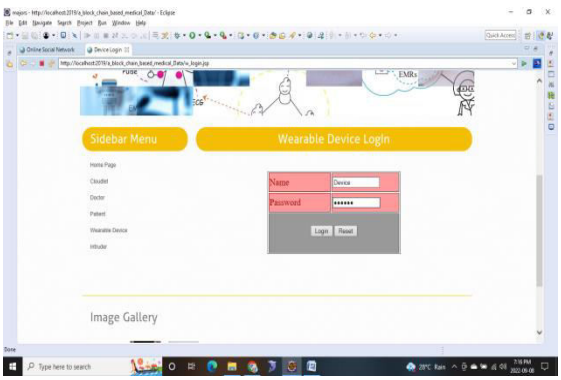
and transmission process as well as locating rogue nodes. To guarantee that our method is lightweight, we make use of an attribute-based signature, often known as an ABS.

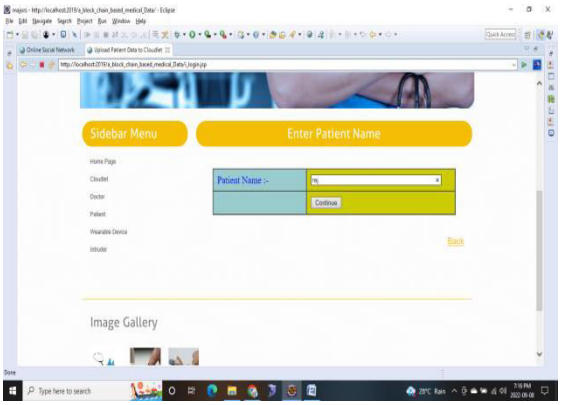
IV RESULTS











V CONCLUSION

To assure the credibility of the data collected in surroundings with fog, we have presented our suggested SBBS. Underpinning ABS makes authentication easier, as was mentioned in this post, and Blockchain makes it possible for us to construct a safe network environment, which helps reduce the likelihood of data being tampered with and enables real-time synchronisation. As part of our effort to establish the usefulness of the proposed method, we also examined its level of safety and performance. Optimisation of the suggested approach for more diversified settings, such as in an antagonistic context (for example, battlefield or military IoT scenarios), is an area of focus for study that will continue inside the coming.

REFERENCES

[1] F. Aït-Salaht, F. Desprez, and A. Lebre, “An overview of service placement problem in fog and edge computing,” ACM Comput. Surveys, vol. 53, no. 3, pp. 1–35, 2020.

[2] F. Bonomi, R. A. Milito, J. Zhu, and S. Addepalli, “Fog computing and its role in the Internet of Things,” in Proc. 1st Ed. MCC Workshop Mobile Cloud Comput., 2012, pp. 13–16.

[3] R. Mahmud, R. Kotagiri, and R. Buyya, “Fog computing: A taxonomy, survey and future directions,” in Internet of Everything. Singapore: Springer, 2018, pp. 103–130.

[4] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.

[5] M. Billinghurst and T. Starner, "Wearable devices: New ways to manage information," Computer, vol. 32, no. 1, pp. 57–64, 1999.

[6] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[7] Z. Hao, E. Novak, S. Yi, and Q. Li, "Challenges and software architecture for fog computing," IEEE Internet Comput., vol. 21, no. 2, pp. 44–53, Mar./Apr. 2017.

[8] K. Hong, D. J. Lillethun, U. Ramachandran, B. Ottenwälder, and B. Koldehofe, "Mobile fog: A programming model for large-scale applications on the Internet of Things," in Proc. 2nd ACM SIGCOMM Workshop Mobile Cloud Comput., 2013, pp. 15–20.

[9] L. Zhang, W. Jia, S. Wen, and D. Yao, "A man-in-the-middle attack on 3G-WLAN interworking," in Proc. IEEE Int. Conf. Commun. Mobile Comput., vol. 1, 2010, pp. 121–125.

[10] A. V. Dastjerdi et al., "Fog computing: Principles, architectures, and applications," in Internet of Things. Cambridge, MA, USA: Morgan Kaufmann, 2016, pp. 61–75.

[11] D. Kovachev, Y. Cao, and R. Klamma, "Mobile cloud computing: A comparison of application models," 2011. [Online]. Available: arXiv:1107.4940.

[12] R. Prodan and S. Ostermann, "A survey and taxonomy of infrastructure as a service and Web hosting cloud providers," in Proc. 10th IEEE/ACM Int. Conf. Grid Comput., 2009, pp. 17–25.

[13] P. T. Endo et al., "Resource allocation for distributed cloud: Concepts and research challenges," IEEE Netw., vol. 25, no. 4, pp. 42–46, Jul./Aug. 2011.

[14] M. Aazam and E.-N. Huh, "Dynamic resource provisioning through fog micro datacenter," in Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom workshops), 2015, pp. 105–110.

[15] Y. Fan, X. Lin, G. Tan, Y. Zhang, W. Dong, and J. Lei, "One secure data integrity verification scheme for cloud storage," Future Gener. Comput. Syst., vol. 96, pp. 376–385, Jul. 2019.

[16] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 9, pp. 1621–1631, Sep. 2012.

[17] Y. W. Law, M. Palaniswami, G. Kounga, and A. Lo, "WAKE: Key management scheme for wide-area measurement systems in smart grid," IEEE Commun. Mag., vol. 51, no. 1, pp. 34–41, Jan. 2013.

[18] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, "Talking to strangers: Authentication in ad-hoc wireless networks," in Proc. NDSS, 2002, pp. 65–82.

[19] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, "A timing-based scheme for rogue AP detection," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 11, pp. 1912–1925, Nov. 2011.

[20] W. Wei, F. Xu, and Q. Li, "MobiShare: Flexible privacy-preserving location sharing in mobile online social networks," in Proc. IEEE INFOCOM, 2012, pp. 2616–2620.

[21] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE INFOCOM, 2010, pp. 534–542.

[22] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, "LT codes-based secure and reliable cloud storage service," in Proc. IEEE INFOCOM, 2012, pp. 693–701.

[23] E. Damiani, S. D. C. D. Vimercati, S. Paraboschi, P. Samarati, and F. Violante, "A reputation-based approach for choosing reliable resources in peer-to-peer networks," in Proc. 9th ACM Conf. Comput. Commun. Security, 2002, pp. 207–216.

[24] Y. Shi, S. Abhilash, and K. Hwang, "Cloudlet mesh for securing mobile clouds from intrusions and network attacks," in Proc. 3rd IEEE Int. Conf. Mobile Cloud Comput. Services Eng., 2015, pp. 109–118.

[25] S. Sarkar, S. Chatterjee, and S. Misra, "Assessment of the suitability of fog computing in the context of Internet of Things," IEEE Trans. Cloud Comput., vol. 6, no. 1, pp. 46–59, Jan.–Mar. 2018.

[26] F. Bonomi, R. A. Milito, P. Natarajan, and J. Zhu, "Fog computing: A platform for Internet of Things and analytics," in Big Data and Internet of Things: A Roadmap for Smart Environments. Cham, Switzerland: Springer, 2014, pp. 169–186.

[27] Y. Fan et al., "SNPL: One scheme of securing nodes in IoT perception layer," Sensors, vol. 20, no. 4, p. 1090, 2020.

[28] W. Liang, W. Huang, J. Long, K. Zhang, K.-C. Li, and D. Zhang, "Deep reinforcement learning for resource protection and real-time detection in IoT environment," IEEE Internet Things J., vol. 7, no. 7, pp. 6392–6401, Jul. 2020.

[29] W. Liang, K.-C. Li, J. Long, X. Kui, and A. Y. Zomaya, "An industrial network intrusion detection algorithm based on multifeature data clustering optimization model," IEEE Trans. Ind. Informat., vol. 16, no. 3, pp. 2063–2071, Mar. 2020.

[30] W. Liang, Y. Fan, K.-C. Li, D. Zhang, and J.-L. Gaudiot, "Secure data storage and recovery in industrial blockchain network environments," IEEE Trans. Ind. Informat., vol. 16, no. 10, pp. 6543–6552, Oct. 2020.