CAN BLOCKCHAIN BE A SOLUTION TO IOT TECHNICAL AND SECURITY ISSUES

Adanma Cecilia Eberendu[1], Titus Ifeanyi Chinebu[2]

[1]Department of Computer Science, Madonna University,
Nigeria Elele Rivers State, Nigeria
[2]Department of Physical Sciences, Federal College of Dental Technology
and Therapy, P. M. B. 01473 Trans Ekulu Enugu, Nigeria.

ABSTRACT

The Internet of Things (IoT) is a growing trend in technology that interconnects millions of physical devices from any location anytime. Currently, IoT devices have become an integral part of human lives, as such organizations are deeply concerned with its security and technical issues. Blockchain system comprises a distributed digital ledger which is shared among community of users on the Internet; validated and recorded transactions in the ledger which cannot be altered or removed. We presented the challenges of IoT devices and how blockchain can be used to alleviate these problems. An outline of how to integrate blockchain with IoT was tackled, highlighting the challenges of IoT and how blockchain can remedy the issues. It was concluded that blockchain has the capability to curb the challenges posed by IoT devices.

KEYWORDS

Internet of things, blockchain, IoT security, technical and security issues, IoT devices.

1. INTRODUCTION

Recent advancements in semiconductor technology have had tremendous impact on solutions that allow for the direct integration of wireless network connectivity in embedded processors, sensors, and actuators. These innovations and advancements have also contributed to increased interest in Internet of Things (IoT) applications. IoT comprises the ubiquitous existence of different objects (mobile telephones, RFID, actuators, sensors, tablets, laptops, etc.) that interact with one another to achieve common objectives [1]. IoT stands for a global network interconnection of everyday things [2], that are uniquely addressable based on some special communication protocols. IoT interconnects people and things anytime, anywhere with anything and anyone using available network and service and involves device that have capability of sensing, actuating and communicating so as to link information and physical world.

The purpose of IoT is to connect things (devices, communication and services) anytime, anywhere with anyone using networks.

Chang et al. [3] discovered that smart devices top the chart for potential IoT deployment. The major factors affecting the adoption of IoT are the will of home users to acquire the devices, security of these devices, and expediency of use [4]. IoT devices are increasing and growing exponentially and this rapid growth has rendered the existing security measures inadequate [5]. Also, scalability due to over-dependence on a cloud server for identification, authentication, and

DOI: 10.5121/ijnsa.2021.13609

connection of smart devices created concerns for security such that an attack on such cloud server involves the entire system.

Arabo [6] explained that there are lots of security and privacy concerns about these IoT devices and appliances despite the benefits associated with them. Razzag et al. [5] reported that consumers spend over $2 trillion annually on IoT devices. Dorri, et al [7] noted that in most cases the user of IoT devices within IoT environments generates good amount of data without the consent of the consumer. IoT devices provide many benefits to consumers but are also vulnerable to attacks. Most of these consumers are not completely aware of the implications of sharing these devices or their personal data, as such, connected devices pose security risk to them. Consumers usually assume that devices and appliances work perfectly well because they rely on devices' default configurations without taking note of the technical manuals and documents. There are some challenging factors that are inherent in IoT – interoperability [8] resource constraints (signalling, bandwidth, power consumption) [9], privacy and vulnerability [10].

One of the causes of security challenges in IoT system is that manufacturers release IoT devices to the market without given consideration to hardware issues, guessable-weak password and unsecure update mechanism. Also, social engineering attacks is the order of the day since most users are unaware of the functionality of IoT devices thereby putting everything at risk. IoT devices updates are not released frequently as new vulnerabilities are discovered, as such most IoT devices are endangered from the time of manufacturing. According to Abdelghaffar and Abousteit [8], lack of standard or the interoperability is the cause of interconnection of objects so that manufacturers can increase market share and then make more profit. Malware also threats and attacks IoT devices by performing unwanted actions without the consent of the consumer thereby resulting in data damages and theft. Some of the threats are device and information modification, data filtering message reproduction, and network or system or device failure [11]. Attacks might be botnet, ransomware, espionage or eavesdropping, rouge devices, etc. According to Dai et al [10], IoT systems are built on a client/server model which may not be able to spread over the system. To move IoT forward, a distributed model that will extend over distributed system is encouraged and blockchain technology which has decentralized capability is needed to expand the IoT. The main problem with IoT is that all devices are connected centrally in form of client/server model where the server authenticate the devices. In other to surmount this problem, blockchain, as a distributed ledger technology provides decentralized approach that will overcome this flaw.

Blockchain has no single vulnerability as such it provides military-based security for IoT devices. It is capable of addressing these security challenges of IoT because users in blockchain maintain a copy of their ledger and authenticate all new contracts communally through an agreed process before accepting them on to the ledger [12].

Blockchain originally known as chain-of-blocks is a group of computers that keeps immutable records of data called distributed ledger or blocks that are linked together using cryptography. It is a time-stamped series of data that entered into the chain at intervals known as blocks with verified transactions and order. Cui et al [11] said that the blocks contain transaction information, such as amount, date and time of purchase, distinctive algorithmic code for differentiating one block from another and identity of each party associated with the transaction. (A blockchain is a distributed tamper-resistant ledger which is readable to certain parties only. Blockchain is a distributed, incorruptible and tamper-resistant ledger that has the potential to address security challenges of IoT, especially on data integrity and reliability [13]. Minoli and Occhiogrosso [14] described blockchain as a cryptographically-linked list of blocks conceived from different points. Blockchain is widely accepted and is mainly used in smart contracts, digital assets, and distributed storage. The purpose of this work is to provide an overview of how blockchain technology can solve inherent challenges of Internet of Things systems. The discussion of how Blockchain's incorporation into IoT would curb the inadequacies of centralization, scalability, security, and privacy concerns will be carried out too.

2. RELATED LITERATURE

The two concepts which are making waves in the technology circle as well as business world are blockchain and Internet of Things (IoT). Jesus et al [15] said that integrating them will revolutionize the way we do things, while Alamri et al [16] pointed out that the two are already on every lip in technological profession and there are more to talk about them. IoT involves the continuous increase in the number of data-gathering devices coming into the business activities or private homes. Blockchain is an encrypted, distributed ledger system drawn to establish tamper-proof, real-time registers. Apart from centralization problem, Dorri, et al [7] identified that most IoT devices have limited resources and privacy issues which makes them less compatible with the requirements of complex automated systems. They proposed a blockchain based solution for the IoT security and privacy issues and to curb the shortcomings of the earlier viewed propositions. They argued that the Blockchain is an effective and efficient technology for tackling issues of security and privacy in IoT. Not with standing, blockchain has issues of bandwidth, latency overheads and scalability. To address these issues, Dorri et al.,[7] used smart home setting to develop lightweight scalable blockchain (LSB) for IoT security and privacy. Atlam, et al., [17] combined blockchain with IoT to accentuate the challenges and expected benefits. They concluded that this combination can considerably resulted new business models and distributed applications because it will allow peer-to-peer messaging, file distribution and autonomous coordination between devices.

Shouran, et al., [18] looked at the security requirements for smart homes in a smart environment and services provided over the wireless network. Kshetri [19] agreed that combining blockchain and IoT will enable IoT devices to carry out autonomous transactions through smart contract and also produce more significant impact with artificial intelligence and big data solution. Dai et al.,[10] outlined the issues associated with IoT and opined that integrating blockchain with IoT will be a perfect solution to inherent problems of IoT. They then proposed blockchain of things (BCoT) with these merits that blockchain-composite layer encourages interoperability among IoT systems. Also, cryptographic mechanisms are characteristics of blockchain that enforces data integrity and each data block in the blockchain has a historic timestamp that enables data traceability. Kouzinopoulos et al., [20] discovered that integrating blockchain into IoT will give organizations a verifiable, secured and permanent method of recording data processed by IoT devices. Hashemi, et al., [21] proposed a BC-based multiple tier IoT architecture that allows data sharing among devices. It comprised three major components: data management protocol, store system and message service. Data management provides a platform for the user (data owner, data requester or source of data), the messaging system increases network scalability using the publish-subscribe model while stores data private use the Blockchain. Duroc and Tedjini [22] suggested that radio frequency identification (RFI) could be used to make this possible. Furthermore, Popescul and Georgescu [23] described a world where every single electronic device or component would be interconnected and other items or object are all labelled with information linked to it. Ibarra-Esquer, et al., [24] identified the tags to allow for the possibility to obtain information in remote and seamlessly contact-less technique. This makes them qualify to be called nodes in the inter-networked physical world that is homologous or similar to the Internet and itemized as another type of Internet of Things.

Also, Skarzauskiene and Kalinauskas [25] were of the opinion that the majority of IoT devices circle around a connected network and this network houses things, objects, and other sensor-based devices to facilitate communication among one another. Trusted IoT alliance (TIoT) [26] was formed by 17 organizations as a working group to integrate IoT and Blockchain in order to solve the problems of security, privacy, reliability, heterogeneity, and flexibility inbuilt into IoT framework [26]. Apart from TIoT many other groups have been formed to look into IoT and Blockchain integration, such as Hyperledger Project, EthEmbeded, LO3ENERGY, and CoT (Chain of Things).

3. BLOCKCHAIN AND IOT ISSUES

Table 1: The Major challenges of IoT

Challenge	Causes
Security. [5], [7], [20], [23], [27]	Changing information from remote devices Using infected devices Inability to keep track of all connected devices on the network IoT devices lack security updates As connected devices increases, endpoint vulnerability increases
Centralization [28], [29], [15], [30]	Identification and authentication of all devices Connected devices exclusively traverse the internet irrespective of their distance Client/Server model – many clients attached to a single server
Transparency [3]	Inaccurate and inaccessible data inventories [31] Unavailability of data confidentiality policy [32]
Interoperability [8], [33], [34]	IoT devices are connected to actual applications, so standardization is difficult. IoT devices framework and the standard does not exist. IoT devices are proprietary-based, highly heterogeneous as to core communication protocols, data formats, and technologies

3.1. Blockchain and IoT Security Issues

According to Sezer [27], security is one of the issues stalling IoT devices from been extensively deployed. Attacks that affect most IoT devices are those that make network resources unavailable to potential users, interrupt communication between systems, spy and cause intrusion that compromises personal data, and infect the botnets with the intention of mining the cryptocurrency of the consumers [12]. One of the major challenges is when numerous computer systems send voluminous requests for data or information to centralized server, thus causing denial of service for clients of the intended system. IoT devices that are not secured give cyber-criminals the opportunity to hack the system and launch distributed denial of service attacks.

Cui et al., [11] said that integrating blockchain into IoT will provide extra security, since blockchain ledger cannot be controlled or corrupted and there is no interception of single thread of communication. Blockchain also provides direct payment services in crypto currencies without any third-party manager; for example, Bitcoin. Therefore, this sovereign security solution makes it a faultless component for IoT solutions.

Blockchain has more robust level of encryption than IoT as such parties cannot overwrite existing records on the network [35]. IoT data stored in blockchain will create additional layer in the IoT security to block cyber-criminals from gaining easy access to the network[36]. Viriyasitavat et al., [34] opined that encryption and distributed storage of blockchain allow securely recording of data in IoT machines as such all detailed transactions are carried out without any human interference. With this the data integrity is preserved and all parties in the supply chain will trust it. Every participant in blockchain technology has a unique identity which is linked to the account and this ensures that the owner operates the transactions. The encryption on blockchain makes it difficult to hack or disturb the traditional setup of the chain [30]. Minors monitor all transactions on the blockchain system, thus maintaining the integrity of the blockchain. For the purpose of security, any block or transaction added to the blockchain program cannot be edited. Hackers have been unable to succeed on attacking or threating blockchain, proving that blockchain is trustworthy, tamper-proof, and resistant to technical failures and malicious attacks [37]. This is achievable through decentralization

3.2. Blockchain and IoT Centralization Issues

The centralized client-server system is a major problem with IoT systems which makes it vulnerable to failure. Blockchain tackles this issue by distributing requests to all devices on the network. Centralization is still one of the hitches experienced by IoT due to the large amounts of data that network of sensors gathered with possibly low processing speeds [32]. The centralized server should be authenticated, authorized, and connect numerous users in the network thereby causing congestion along the line. In order to overcome this, Alam [28] suggested that organization have to invest huge amount into the centralized server that can accommodate the massive amount of data or information flow expected within the network. IoT network can handle transactions across various devices from different organizations, if any attack occurs it becomes difficult to trace the source of information leakages [15]. Also determining the owners of the generated data is always difficult.

According to Popescul and Georgescu [23], in IoT technology, a hacker only needs access to the server with the information in order to add, modify and delete any data. Data in blockchain is shared among nodes. Distributed system will disseminate accepted legal amendments of new information among other parties in the network. When processing large requests, the server in IoT network can breakdown while distributed-ledger is significantly resistant to pressure on the network because the requests are distributed on the whole network rather than on a particular node[38]. The failure of the server in IoT network causes failure to the entire network, thus inconveniencing the parties but the blockchain network has large number of connected devices, as such failure may not occur unless the capacity of the devices is higher than that of the network. Ghuli et al.,[39] discovered that the connection with the server in IoT network can be problematic when the server is located remotely, blockchain network allows the client to choose any path to follow and disseminate the required information. IoT Server has the duty of storing all data, receiving request, amending, updating and deleting data and the load might exceed the limit during peak period [31]. All clients are connected to the server which has limited capacity, finite resources and traffic in the IoT network. Therefore, scaling vertically up after the limit will decrease the performance drastically even with increase in hardware and software capabilities. Blockchain shares its load among several participants. Blockchain allows trusted data to be pooled and shared directly among participants without intermediaries, thereby eliminating third-party in the value chain transaction. Mohanta et al., [40] opined that with blockchain's smart contract, IoT devices automate payments and transactions across different devices. Blockchain keeps track of unchangeable historical records of IoT devices and this improves the performance of IoT devices on the network without centralization. Organizations can store smart contracts in the blockchain to allow the execution of contractual arrangements among parties provided they satisfy laydown criteria. For instance, automatic authorization of contract payment without third party intervention [34]. In blockchain technology, transaction data is distributed across a chain of multiple devices, and there is no specific managing node. Single point of vulnerability or failure does not exist, and so data are highly resistant to hacking, theft, and forgery[41]. Failure of a single node does not affect the functionality of other nodes on the network. Participants are dependent on blockchains for not relying on a single node throughout the transaction process. As soon as the participants agree on a transaction, the system proffers the information to other network nodes instead of a single server as the case of traditional transaction systems [39]. Thus, preventing cyberattacks, theft, and other malicious crimes as the transaction is openly distributed. Decentralized capability of blockchain eliminates the need for third-party through verification and validation mechanisms[19]. Blockchain distributed ledger records each transaction in a way that they are available to all blockchain participants. So, the ledgers are shared publicly, creating transparency and trust in the whole system. Thus, blockchain technology monitors all transaction data and almost indecipherable to fraud.

3.3. Blockchain and IoT Transparency Issues

Transparency is one of the capabilities of Blockchain that allows authorized parties to access the network and track previous transactions. With this, data leakages can easily be identified and remedial action taken immediately before hackers take advantage of it [17]. The transparent nature of blockchain records enables authorized parties to track and analyse ongoing network activities. Organizations generate huge data transactions among multiple networks, immutable ledger record as a protector tracks data or goods along the nodes in the supply chain [41]. Blockchain secures the data from IoT sensors thereby making blockchain a more useful ledger. The nodes in blockchain technology are similar to the objects in IoT system, thus making connected objects more secured and reliable. Blockchain-based IoT systems simplify business transactions thereby enhancing transparency for better client experience. Ibarra-Esquer et al., [24] agreed that integrating blockchains into IoT network enables secure distrusted messaging among devices on a network, so blockchain handles messages in the same way it handles financial transactions on Bitcoin network. The ability of blockchain to offer smart contract-based networks (e.g. Ethereum) allows IoT devices to interconnect and trade with one another confidently that the transaction will be treated according to the predefined rules of engagement. With distributed ledger capability of blockchain system no one can interfere with blockchain transactions, as such trust among the stakeholders are eliminated [37]. Blockchain processes large volume of transactions faster than IoT system and can manage millions of connected devices even when the number increases [20]. Inbuilt trust in blockchain allows organizations to reduce costs of processing overheads related to IoT gateways such as communication or hardware overhead [19]

3.4. Blockchain and IoT Interoperability Issues

Interoperability occurs when two or more heterogeneous systems or devices on the networks communicate with each other to attain a common purpose [33]. IoT systems and devices are disintegrated and cannot share their data with each other due to lack of communication protocols, data formats, and technologies [42]. This means that data cannot be switched across interconnected devices. Many IoT devices are still designed to work on a predefined hardware configuration, so they hinder effective incorporation of new devices that can attack other operational issues. According to Amjad et al.,[43], IoT devices experience interoperability challenges when they communicate services to the cloud or combining data or information from different devices. Interoperability can also be undermined when different devices reuse services generated by another IoT device [8].With the aid of cross-chain technology, blockchain has the ability to share information across different systems, devices and networks. Cross-chain technology focuses on chain interoperability across private networks or between public blockchains and private networks [42]. Blockchain also uses tools like atomic swaps and multi-chain protocols to facilitate interoperability.

3.5. Stability Strengths of Blockchain

If a block has been approved, it will be difficult to reverse, which means that all registered data into the blockchain are extremely hard to eliminate or modify [15]. Blockchain technology stores transaction data where an audit trail is required so as to track every modification and permanently keep a record on a distributed and public ledger. Blockchain is designed to easily locate and correct any problem and also creates an irreversible audit trail [36]. Also, distrustful transaction cannot be hidden. It is no longer necessary to create multiple ledgers for various participants, one stable ledger is distributed among all participants with least deceitful activities [14].

3.6. Scalability in Blockchain and IoT

IoT device is said to be scalable when it has the ability to agree with the changes within its environment and future requirements [38] while in blockchain scalability means that the system has high transaction per second than other systems. It is an important quality of systems with the capability of handling growing amount of work [44]. In blockchain, scalability means that the platform supports increasing load of transactions, in addition to the increasing number of nodes within the network. IoT scalability. Blockchain system is distributed and verification of transactions in each node is significant. The number of transactions in each node is regulated. According to Reyna et al., [29], it might take a user several hours to complete a procedure as such it is impractical to increase the number of active participants due to the transaction speed. The more participants join the blockchain network, the slower the transaction speed. Blockchains are as scalable as centralized system, so blockchain completes transaction depending on the congestion of the network [34]. In order to solve the scalability problem of blockchain, researchers suggested performing transactions outside the blockchain, and then store and access information in it. Also, approved networks can be used to solve the problem of scalability in blockchain technology. Scalability is necessary to achieve success of the IoT[45]. Scalability can be overwhelmed through efficiency, robustness, and standardization services on the device,.

4. CONCLUSION

In conclusion, blockchain and IoT are new trends in technologies with huge potential, however, companies are skeptical of adopting them due to technical and security reasons. Though some are combining them to ascertain the possibility of minimizing the security and other associated business risks, Blockchain and IoT will continue to develop into globally acceptable standard. There might be challenges along the line but more businesses are leveraging into blockchain-based IoT systems.

Finally, blockchain will pave way for a lot of possibilities to implement IoT system. Despite these few drawbacks, blockchain technology presents some unique benefits though its adoption in the industry still have a long way.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito. "The internet of things: A survey." *Computer networks* Vol. 54 No.15. 2010 pp. 2787-2805.

[2] F. K. Santoso and N. CH Vun. "Securing IoT for smart home system." In *2015 international symposium on consumer electronics (ISCE)*, pp. 1-2. IEEE, June. 2015.

[3] Y. Chang, X. Dong, and W. Sun. "Influence of characteristics of the Internet of Things on consumer purchase intention." *Social Behavior and Personality: an international journal* vol. 42, no. 2 March, 2014: pp 321-330.

[4] L Sang-Hyun, J. G. Lee and M. Kyung-Il. "Smart home security system using multiple ANFIS." *International Journal of Smart Home* vol 7. no.3. May 2013: pp. 121-132.

[5] M. Razzag, H. Gill, S. Ullah, and M. Qureshi. Security Issues in the Internet of Things (IoT): A Comprehensive Study. *International Journal of Advanced Computer Science and Application, vol. 8. No. 6* 2014. pp.383-388

[6] A. Arabo. "Cyber security challenges within the connected home ecosystem futures." *Procedia Computer Science* vol. 61 Jan. 2015: pp. 227-232.

[7] A. Dorri, S. S. Kanhere, R.Jurdak, and P.Gauravaram. "Blockchain for IoT security and privacy: The case study of a smart home." In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*, March. 2017. pp. 618-623. IEEE.

[8] H. Abdelghaffar and M. Abousteit. "Internet of Things (IoT) Interoperability Success Criteria." *International Journal of Enterprise Information Systems (IJEIS)* vol. 17, no. 1 Jan. 2021: pp. 85-105.

[9] A. S Pradeep, T. W. Yiu, and R. Amor. "Leveraging blockchain technology in a BIM workflow: A literature review." In *International Conference on Smart Infrastructure and Construction 2019 (ICSIC) Driving data-informed decision-making*, 2019. pp. 371-380. ICE Publishing.

[10] Y. Dai, D. Xu, K. Zhang, S. Maharjan, and Y. Zhang. "Deep reinforcement learning and permissioned blockchain for content caching in vehicular edge computing and networks." *IEEE Transactions on Vehicular Technology* vol. 69, no. 4. February, 2020: pp. 4312-4324.

[11] P. Cui, U. Guin, A. Skjellum, and D. Umphress. "Blockchain in IoT: current trends, challenges, and future roadmap." *Journal of Hardware and Systems Security* vol.3, no. 4. Dec. 2019: pp. 338-364.

[12] A. P. Joshi, M. Han and Y. Wang. "A survey on security and privacy issues of blockchain technology." *Mathematical foundations of computing* vol.1, no. 2. 2018. p. 121.

[13] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J Guo, X Niu, and K Zheng. "Survey on blockchain for Internet of Things." *Computer Communications* vol. 136. February, 2019: pp.10-29.

[14] D.Minoli, and B. Occhiogrosso. "Blockchain mechanisms for IoT security." *Internet of Things* Vol. 1 Sep, 2018: pp. 1-13.doi:10.1016/j.iot.2018.05.002

[15] E. F. Jesus, V. R.L Chicarino, C.V.N De Albuquerque, and A A. de A. Rocha. "A survey of how to use blockchain to secure internet of things and the stalker attack." *Security and Communication Networks* April, 2018.

[16] M. Alamri, N. Z. Jhanjhi, and M. Humayun. "Blockchain for Internet of Things (IoT) research issues challenges & future directions: A review." *Int. J. Comput. Sci. Netw. Secur* vol. 19 May, 2019: pp. 244-258.

[17] H. F. Atlam, A.Alenezi, M. O. Alassafi, and G. Wills. "Blockchain with internet of things: Benefits, challenges, and future directions." *International Journal of Intelligent Systems and Applications* vol. 10, no. 6. 2018: pp. 40-48.

[18] Z. Shouran, A.Ashari and T.Priyambodo. "Internet of things (IoT) of smart home: privacy and security." *International Journal of Computer Applications* vol. 182, no. 39 February, 2019: pp. 3-8.

[19] N. Kshetri, “Can blockchain strengthen the internet of things?" *IT professional* vol. 19, no. 4 August, 2017: pp. 68-72.

[20] C.S. Kouzinopoulos, G. Spathoulas, K. M. Giannoutakis, K. Votis, P. Pandey, D. Tzovaras, S. K. Katsikas, A. Collen, and N. A. Nijdam. "Using blockchains to strengthen the security of internet of things." In *International ISCIS Security Workshop*, February, 2018pp. 90-100. Springer, Cham.

[21] 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)*, 2016.pp. 13-24. IEEE,

[22] Duroc, Yvan, and SmailTedjini. "RFID: A key technology for Humanity." *ComptesRendus Physique* vol. 19, no. 1-2 Jan, 2018: pp. 64-71.

[23] M. Georgescu, and D, Popescul, Security, privacy and trust in internet of things: A straight road? *International Business Information Management Association, IBIMA*. 2015.

[24] J. E. Ibarra-Esquer, F. F. González-Navarro, B. L. Flores-Rios, L. Burtseva, and M A. Astorga-Vargas. "Tracking the evolution of the internet of things concept across different application domains." *Sensors* vol. 17, no. 6 June, 2017: p. 1379.

[25] A. Skaržauskienė, and M. Kalinauskas. "The internet of things: when reality meets expectations." *International Journal of Innovation and Learning* 17, no. 2. Jan. 2015: pp. 262-274.

[26] V.K. Aggarwal, N. Sharma, Ila Kaushik, and B. Bhushan. "Integration of Blockchain and IoT (B-IoT): Architecture, Solutions, & Future Research Direction." In *IOP Conference Series: Materials Science and Engineering*, vol. 1022, no. 1, 2021.p. 012103. IOP Publishing,

[27] S. Sezer. "T1C: IoT Security: -Threats, Security Challenges and IoT Security Research and Technology Trends." In *2018 31st IEEE International System-on-Chip Conference (SOCC),* September, 2018. pp. 1-2. IEEE.

[28] T. Alam. "Blockchain and its Role in the Internet of Things (IoT)." *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* vol. 5, no. 1. 2019.

[29] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz. "On blockchain and its integration with IoT. Challenges and opportunities." *Future generation computer systems* vol. 88 Nov., 2018: pp.173-190.

[30] S. Sahraoui, and A. Bilami. "Compressed and distributed host identity protocol for end-to-end security in the IoT." In *2014 International Conference on Next Generation Networks and Services (NGNS),* 2014. pp. 295-301. IEEE.

[31] A. Pal, H. K. Rath, S. Shailendra, and A. Bhattacharyya. "IoT standardization: The road ahead. Internet of Things - technology, applications and standardization.". 2018. doi:10.5772/intechopen.75137.

[32] A. Al Sadawi, M. S. Hassan, and M. Ndiaye. "A Survey on the Integration of Blockchain with IoT to enhance performance and eliminate challenges." *IEEE Access* vol. 9 April, 2021: pp. 54478-54497.

[33] H. Derhamy, J. Eliasson, and J. Delsing. "IoT interoperability—on-demand and low latency transparent multiprotocol translator." *IEEE Internet of Things Journal* vol. 4, no. 5 April, 2017: pp. 1754-1763.

[34] W. Viriyasitavat, T. Anuphaptrirong, and D. Hoonsopon. "When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities." *Journal of industrial information integration* vol. 15 September, 2019: pp. 21-28.

[35] S. Roy, M. Ashaduzzaman, M. Hassan, and A. R. Chowdhury. "Blockchain for IoT security and management: Current prospects, challenges and future directions." In *2018 5th International Conference on Networking, Systems and Security (NSysS)*, December, 2018: pp. 1-9. IEEE.

[36] U. Tariq, A. Ibrahim, T. Ahmad, Y. Bouteraa, and A. Elmogy. "Blockchain in internet-of-things: a necessity framework for security, reliability, transparency, immutability and liability." *IET Communications* vol. 13, no. 19. December, 2019: pp. 3187-3192.

[37] Y. Yu, Y. Li, J. Tian, and J. Liu. "Blockchain-based solutions to security and privacy issues in the internet of things." *IEEE Wireless Communications* vol.25, no. 6 Dec. 2018: pp.12-18.

[38] S. Arif, M. A Khan, S U Rehman, M A Kabir, and M Imran. "Investigating smart home security: Is blockchain the answer?" *IEEE Access* vol. 8 June, 2020: pp. 117802-117816.

[39] P. Ghuli, U P Kumar, and R Shettar. "A review on blockchain application for decentralized decision of ownership of IoT devices." *Advances in Computational Sciences and Technology* 10, no. 8. 2017: pp. 2449-2456.

[40] B.K. Mohanta, S S. Panda, and D. Jena. "An overview of smart contract and use cases in blockchain technology." In *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, July, 2018.pp. 1-4. IEEE,

[41] Y. Lee, S. Rathore, J H Park, and J H Park. "A blockchain-based smart home gateway architecture for preventing data forgery." *Human-centric Computing and Information Sciences* vol. 10, no. 1 Dec., 2020: pp. 1-14.

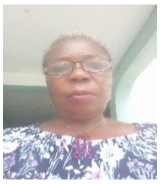
[42] M. Noura, M.Atiquzzaman, and M Gaedke,. Interoperability in Internet of Things: Taxonomies and Open Challenges. *Mobile Network Application* vol.24, 2019: pp.796–809 https://doi.org/10.1007/s11036-018-1089-9

[43] A.Amjad, F. Azam, M. W Anwar, and W H Butt. "A Systematic Review on the Data Interoperability of Application Layer Protocols in Industrial IoT." July, 2021. *IEEE Access*

[44] A. Gupta, R. Christie, and P. R. Manjula. "Scalability in internet of things: features, techniques and research challenges." *Int. J. Comput. Intell. Res* 13, no. 7. 2017: pp.1617-1627.

[45] S. Li, L D Xu, and S. Zhao. "The internet of things: a survey." *Information Systems Frontiers* vol.17, no. 2 April, 2015: pp. 243-259.

AUTHORS



Adanma Cecilia Eberendu is a Senior Lecturer at Madonna University, Nigeria. She received the Ph.D. degree in Software Project Management and her research area is focused on software vulnerability. She has published many articles on software projects management and software vulnerability. She teaches courses in of Software Engineering, Cyber Security and Forensics. She is the corresponding author of this article and can be reached on aceberendu@gmail.com

Titus Ifeanyi Chinebu received the B.Sc.Ed degree in Education/Mathematics, M.Sc. and Ph.D. degrees in Mathematical Modeling from the Department of Mathematics, University of Nigeria Nsukka. From 2013 to 2020 he was a lecturer with the Madonna University Nigeria, Elele Rivers State. He is currently a lecturer in the Department of Applied Sciences, Federal College of Dental Technology and Therapy, Trans Ekulu, Enugu. His research includes Epidemiological Modeling, Biomathematics, Computational Mathematics, Computer/Mobile Malware Model and Financial Mathematics. He has over 18 publications