Library Progress International
Vol.44 No.3, Jul-Dec 2024: P.4432-4438

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Empirical Analysis of Blockchain Based Security for the Internet of Things in Enhancing the Future Technology Using Structural Equation Model Approach.

Mohit Tiwari[1] Tripti Tiwari[2] Prateek Bhatia[3]

[1] Dept of Computer Science and Engineering,
Bharati Vidyapeeth College of Engineering, New Delhi
mohit.tiwari@bharatividyapeeth.edu
[2]Dept of Management Studies,
Bharati Vidyapeeth (Deemed to be University) Institute of Management & Research, New Delhi
tripti.tiwari@bharatividyapeeth.edu
[3]Dept of Computer Science and Engineering,
Bharati Vidyapeeth College of Engineering, New Delhi
prateekbhatia1999@gmail.com

How to cite this article: Mohit Tiwari, Tripti Tiwari, Prateek Bhatia (2024). Empirical Analysis of Blockchain Based Security for the Internet of Things in Enhancing the Future Technology Using Structural Equation Model Approach.. *Library Progress International,* 44(3), 4432-4438.

ABSTRACT

Recent technological advances have made it possible for businesses, individuals, and other groups to completely transform how interconnectedness and corporate activities are carried out. This is known as the Internet of effects. The rise of the Blockchain model made it possible to improve IoT-based future technology in a practical way. Blockchain implementations typically offer additional robust safeguards against data leaks and manipulation, restrict access to relevant information, and facilitate faster data transfer via encrypted networks and connections. The rise of smart homes leads to improved terrain and equitable development and growth. They also help the government regulate pollution, enable energy savings, facilitate smarter transportation, and foster smart diligence.

As a result, several experimenters have claimed that the way Blockchain functions provides a foundation for security support when developing emerging technologies like IoT. The research presented here aims to close the gaps and address important IoT security-related challenges. It also supports the advancement of new technologies that will enhance data analysis, enhance information flow, and help key stakeholders make informed decisions. In order to conduct the study, the experimenters typically employ both primary and secondary data. They gather information from respondents via a check system, analyze it using AMOS statistical software, and draw the proper conclusion from the results.

Keywords— Structural equation model, correlation analysis, blockchain technology, and IoT.

Introduction

Increasing communication between different bias, detectors, and other features that promote progress and advancement has been made possible in large part by the way the IoT operates. IoT is thought to use internet services and colorful smart bias to help meet the unique situations of individualities, businesses, governments, and other assiduity worldwide. This has led to the provision of improved and inventive results. (1). According to some, IoT is becoming an increasingly important part of daily life and may be felt along the vibrant corridors of mortality. In general, it has been noted that although Internet of Things-enabled resting operations can greatly enhance people's overall quality of life, there are a number of challenges related to system configuration at startup, storage of information, operation, sequestration aspects, and accessibility control. Seeing these obstacles as a chance to solve real-world issues and improve resilience in general is one way to approach them (2). Blockchain is described as a largely open-source technology that lowers the overall challenge of lethal crimes and offers stakeholders and addicts from end to end decentralization on safety-related concerns (3). In addition to offering

improved protection against any cyberattacks, it could be crucial for gaining access control. The creation of cryptocurrency was the main objective of the model's inception a decade ago, since it would allow for the storage, updating, and documentation of vital data. The decentralized nature of blockchain technology, which maintains information integrity through related agreement mechanisms, is its main characteristic. It is not necessary to monitor third-party access and trust is established by narrating the public the story, offering reassurance, and disseminating the transaction in a unique way. In the same way that blockchain technology gave the Internet of Things security, researchers have been diligently working to enhance the IoT's general features and usefulness for exciting reasons to provide people's daily lives new development and significance (4). Sustainable development is therefore made possible by the truly low prices at which these biases are currently available. Thanks to additional advancements made feasible by the use of the blockchain relies security in the Internet of Things, people and enterprises' lives may now go more smoothly. Blockchain technology provides additional control and coverage over the functioning of intelligent detectors, colorful technical bias protection, and security-related factors. According to a number of experimenters, the blockchain's integration and operation through IoT bias have helped to generate a harmonious story that is shared throughout the distributed network and have effectively supported each trade's verification (5). This offers substantial advantages for managing the total access control systems. Within the IoT framework, the primary benefits of blockchain-based safety measures are their efficient resource management, assistance with scalability, appropriate access and rights transfer, and criterion operation. They additionally aid in enforcing stricter authorization enforcement (6). Additionally, Blockchain technology facilitates the development of trust chains for improved data operation while also accelerating and fine-tuning the flow of data and information. Authorization enforcement is regarded as a specialized service that is made to fit the needs and tastes of the final consumers. This is seen to be an essential part of making the system for controlling access even stricter and encouraging suicide. Moreover, it is noteworthy that the experimenters have successfully combined cutting-edge and innovative blockchain technology in order to improve the IoT bias's long-term access control system. Two examples of technologies that help improve total control of access are machine learning and deep knowledge techniques, which help by comprehending various patterns and efficiently improving network structure (7). The IoT could benefit greatly from the integration of Blockchain technology, particularly in terms of improved security, interoperability, and network scalability.

In order to progress future technologies, the study aims to critically examine the blockchain relies security of the IoT. Three main topics are covered in this paper: scalability, improved resource management, and transfer of access rights.

1. Review of literature

Transfer of access control from one device to another is important since it allows some access with specific access credentials. For instance, conservation—also known as the transfer of rights of access between various realities—can be performed by a trained auto handyman per the owner's instructions. The thing which grants access to information is referred to in the context of delegation as a representative, while the actuality that requests admission privileges is called the deputy. In massive, extremely mobile networks such the Internet of Things, outsourcing is necessary to give varied, accurate, and flexible access to cash. This allows drug dealers to share information in an organized manner (8). However, it's tricky to create an entire set of pre-defined trusted access control applications centrally for an Internet of Things system.

There are many different types of smart bias when it pertains to IoT security, and they provide drug dealers and other systems bias with a variety of services. IoT systems need to guarantee efficient use, distribution, and sharing of computer and storage resources. Furthermore, drug users seek simple accessibility to such funds, this provides them with exact possession of the assets they need in a dispersed, safe environment (9). In the near future, means will operate rather insufficiently, necessitating an adjustment in resource operation conditions. It is important to create an efficient resource operation framework with a high IoT bias in order to accomplish this. Blockchain technology provides an IoT access control architecture that is more flexible and adaptive in terms of managing resources, making it a viable substitute for more established central access control solutions (10). Remember, blockchain is made up of multiple IoT biases and detaches power from one central node while providing more resource operations flexibility for different scripts, like force chains, power, and transportation. Under these circumstances, the implementation of a blockchain via intelligent contracts mysteriously guarantees the deep and irretrievable data sections (11).

The primary goal of the suggested architecture is to provide trustworthy policy operation and safe communication between next-generation IoT bias, for example, enabled by the underlying blockchain capabilities, transparency, controllability, and scalability. Because of its hierarchical nature, the private blockchain enables more comprehensive authorization in a range of access circumstances (including blockchain location and stoner access)

(12). The stoner posture utilizes cryptographic operations. At the block chain level, light authorization mechanisms are used in accordance with different IoT access control needs. Large numbers of IoT bias can be handled by the suggested armature, which also offers a distributed control of access function that links many IoT bias.

2. Methodology

In order to better understand how Blockchain technology supports safety and additional relevant using IoT devices, for their investigation, the researchers intend to employ a design based on quantitative data (13). The closed-ended questionnaire is used by the researchers to collect primary data, which is the information that is required from the respondents. Utilizing the convenience sampling approach, a representative sample of 181 has been selected by the investigator. To comprehend the results of earlier research in this field, secondary information is used. The inquiry comprises generating critical examinations and path analyses utilizing the collected data and AMOS software (14).

- Study Questions

- Can the use of technology based on blockchain enhance resource management, which enhances security for the IoT?
- Does technology based on blockchain support the safety of Internet of Things devices by efficiently managing access rights?
- In the future, would blockchain provide greater scaling and adaptation for Internet of Things devices?

3. critical analysis and interpretation

This study segment involves critically analyzing the information gathered from the respondents; the main analyses include Chi square, regression analysis, and percentage rate analysis.

Blockchain technology is affordable	**Frequency**	**Percentage**
Strongly Disagree	18	9.9
Disagree	9	5
Neutral	18	9.9
Agree	69	38.1
Strongly Agree	67	37
Total	181	100

Table 1: Blockchain technology is affordable

Based on the comprehensive study, 38.1% of respondents believed with the statement and 37% strongly agreed that it is cost-effective to use Blockchain technology to enhance IoT device security. These results indicate a sizable portion of responders who think that using Blockchain technology is highly productive and supports lowering operating costs.

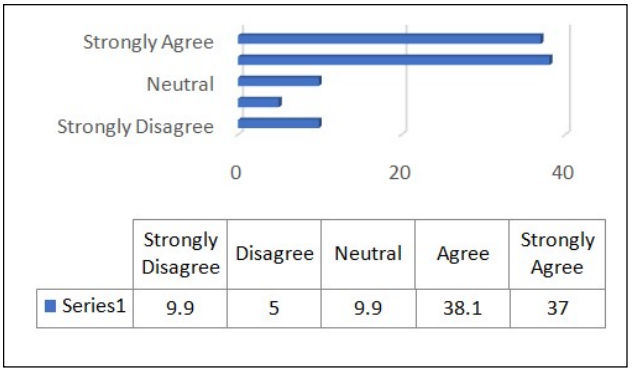

Chart 1: Blockchain is cost effective

Assistance with obtaining permissions	Frequency	Percentage
Strongly Disagree	14	7.7
Disagree	23	12.7
Neutral	4	2.2
Agree	63	34.8
Strongly Agree	77	42.5
Total	181	100

Table 2: Assistance with obtaining permissions

The next study is about understanding how Blockchain technology might support permission enforcement more effectively. This facet is of utmost importance as it permits the evaluation of policy management flexibility concerning data and information flow via Internet of Things devices. About 42.5% of those surveyed firmly believe that blockchain technology helps the augmentation of permissions, and 34.8% of respondents also concur.

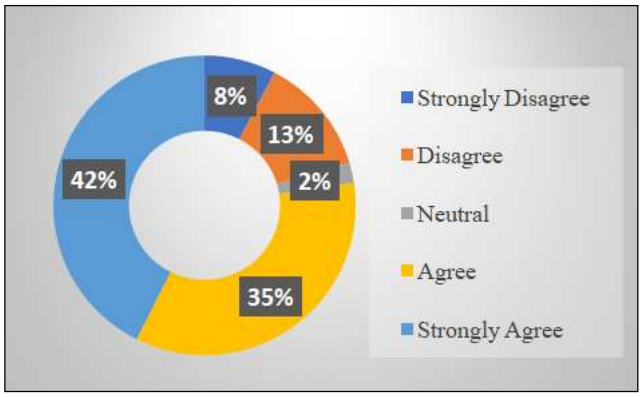

Chart 2: Assistance with obtaining permissions

4. correlation analysis

Another part offers a thorough description of how the relationship between the variables was calculated, simplifying the analysis of the type of relationship that exists among the two kinds of components.

	Improved Resource Utilization	Access Permit	Scalability	Blockchain based security for IoT
Improved Resource	1	0.889	0.826	0.862

Utilization				
Access Permit	0.889	1	0.859	0.87
Scalability	0.826	0.859	1	0.825
Blockchain based security for IoT	0.862	0.87	0.825	1

Table 3: Correlation Analysis

A measure of the connections between both the dependent and independent components is larger than 0.8000, which indicates a significant positive relationship between the factors, as can be seen from the information provided in Table 3 of the statistical analysis. The highest score is 0.870, which is the result of providing improved access rights and managing blockchain for IoT. Better resource operation comes in second with a score of around 0.862 & scalability at 0.825, which Thus, it can be said that every element continues to possess a significant impact on blockchain technology within the IoT.

5. model of Structural equation

This section entails creating an analysis of paths and capturing the research topic that has been formulated by the investigators. SEM is a crucial model that integrates regression analysis and factor styles to comprehend the overall comparison of the components.

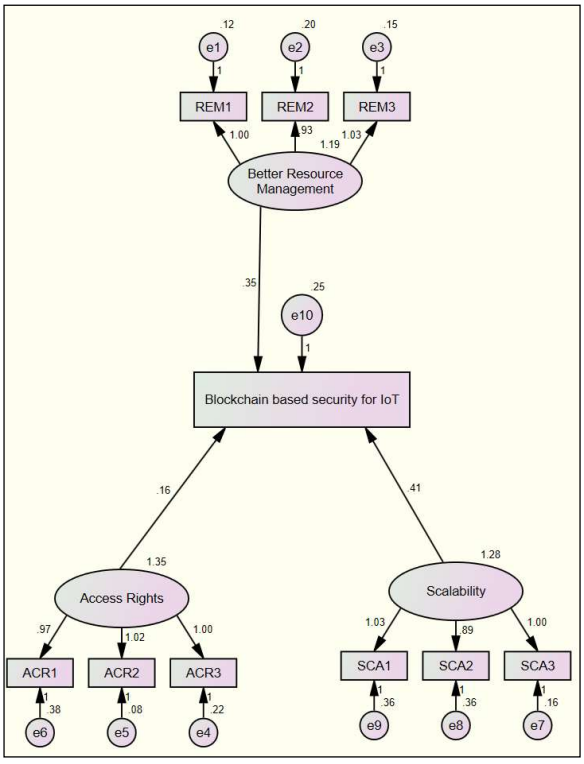

Figure 3: Path analysis using the SEM model

The route analysis that was previously shown shows that the dependent as well as independent variables are still positively correlated.

Reliance Variable	Separate variable	Estimates	Std. Err.	P Coef
Blockchain	Improved	3.94	2.66	0.001

	Resource Utilization			
Blockchain	Access Permit	3.25	2.17	0.00
Blockchain	Scalability	0.58	2.22	0.00
Model Fit	GFI	RFI	CFI	PCFI
Default	0.817	0.881	0.93	0.62

Table 4: SEM analysis and output

The table above displays the p coef. The alternative thesis is considered because there are no variables that are greater than 0.05. Similar to this, the example is regarded as having a voguish fit, as seen by the primary measures such as PCFI (0.62), RFI (0.881), CFI (0.930), and GFI (0.817), which all relate to relative fit.
The way enterprises and other aspects interact has been transformed by associations, individualities, and more thanks to the new miracle of the Internet product operation. The Blockchain approach will enable future IoT-based technology to be upgraded in an efficient manner. Better security against data leaks, access blocking, and information poofing is generally provided by blockchain operations. It also facilitates speedy data transfer over the network and secure connections. The advent of smart homes will lead to better development and terrain, as well as assist governments conserve energy, regulate pollution, build more intelligent transportation, & encourage smart diligence (15). The IoT is believed to leverage a range of ingenious Internet-based goods and assistance to generate superior and more creative outcomes to fulfill the various needs of people, groups, authorities, as well as other astuteness globally. IoT is present in many areas of human activity and is gradually losing its status as an inconsequential aspect of daily life. It is important to note that, in general, Internet of Things-based activities are constantly bringing about groundbreaking advances to raise the standard of living for everyone. However, they also offer colorful configuration issues, a systems overview, storing data, operations, security of data, and access control aspects (16). One way to approach these difficulties is as a chance to improve sustainability in general and solve pressing issues.

The blockchain-based security assistance operation, according to a number of experimenters, intends to advance Internet of Things technologies going forward. This investigation will focus on comprehending the potential and resolving significant security concerns related to the Internet of Things. Additionally, it will support the creation of fresh technologies that will enhance information flow, facilitate data analysis, and help important stakeholders make defensible judgments. The main goal of the concept, which was unveiled in the last ten years, was to create a cryptocurrency that would make it possible to gather, organize, and store important data. The decentralized model of the blockchain is essential because it applies appropriate donation procedures to preserve the information's integrity. The public a guide, which ensures trade dispersion in a creative environment, fosters confidence without the need for a third-party accessibility monitoring system.

6. conclusion

The Internet of Things has seen further advancements that improve people's and businesses' lives as a result of the adoption of blockchain technology, which requires security. Blockchain technology protects various technological devices and security aspects while enhancing administration and monitoring of smart detector use. Several researchers found that by integrating and using blockchain technology via Internet of Things devices, it is feasible to create a reliable system that will be pooled in a manner that is distributed and would enable effective control of individual transactions. When managing all access control systems, this offers a number of major advantages. Surprisingly, the primary outcomes of safety protocols for the IoT, utilizing digital ledger industry is thought to have evolved appropriate resource management, scalability, management of distribution, and exact privileges and access to broadcast. Furthermore, by facilitating information flow and enhancing data accuracy and speed, the Blockchain supporting app contributes to the development of a trustworthy chain that enhances data management. A special service created to satisfy criteria and pricing schedules is license maintenance.

7. references

[1] Gabillon, R. Gallier and E. Bruno, (2020). "Access controls for IoT networks", Social Netw.Comput. Sci., vol. 1, no. 1, pp. 1-13, Jan. 2020. Available: https://doi.org/10.1007/s42979-019-0022-z

[2] Di Pietro, X. Salleras, M. Signorini, and E. Waisbard, (2018).“A blockchain-based trust system for the internet of things,” in Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies, ser. SACMAT ’18. New York, NY, USA: Association for Computing Machinery, 2018, p. 77–83. [Online]. Available: https://doi.org/10.1145/3205977.3205993

[3] Ouechtati, N. B. Azzouna and L. B. Said, (2018). "Towards a self-adaptive access control middleware for the Internet of Things", Proc. Int. Conf. Inf. Netw. (ICOIN), vol. 1, pp. 545-550, Jan. 2018. Available: https://www.researchgate.net/publication/374384619_Empirical_Analysis_of_Blockchain_Based_Security_for_the_Internet_of_Things_Using_Structural_Equation_Model_Approach

[4] Luo, Q. Shen and Z. H. Wu, (2019). "PML: An interpreter-based access control policy language for Web services", CoRR, vol. abs/1903.09756, 2019. Available: https://arxiv.org/pdf/1903.09756

[5] Wu and J. Liang, (2021). "A blockchain-based trust management method for internet of things," Pervasive and Mobile Computing, vol. 72, p. 101330, 2021. Available https://doi.org/10.1016/j.pmcj.2021.101330

[6] Pal, M. Hitchens, V. Varadharajan, and T. Rabehaja, (2019)."Policy-based access control for constrained healthcare resources in the context of the internet of things," Journal of Network and Computer Applications, vol. 139, pp. 57 – 74, 2019.[Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804519301377

[7] Da Xu, Y. Lu, and L. Li, (2021). "Embedding blockchain technology into iot for security: A survey," IEEE Internet of Things Journal, pp. 1–1, 2021. Available https://e-tarjome.com/storage/panel/fileuploads/2021-07-28/1627452809_E15540.pdf

[8] Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, and D. O. Wu, (2020). "Edge computing in industrial internet of things: Architecture, advances and challenges," IEEE Communications Surveys Tutorials, pp. 1–1, 2020. Available: https://ieeexplore.ieee.org/document/9139976

[9] Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, (2019). "Smart contractbased access control for the internet of things," IEEE Internet of Things Journal, pp. 1–1, 2019. Available: https://ieeexplore.ieee.org/document/8386853

[10] A. Baktyan and A. T. Zahary, (2018)."A review on cloud and fog computing integration for iot: Platforms perspective," EAI Endorsed Transactions on Internet of Things, vol. 4, no. 14, 12 2018. Available: https://doi.org/10.4108/eai.20-12-2018.156084

[11] Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, (2018). "Blockchain and iot integration: A systematic survey," Sensors, vol. 18, no. 8, 2018.[Online]. Available: http://www.mdpi.com/1424-8220/18/8/2575

[12] A. Jain, A.K.Yadav& Y. Shrivastava (2019), "Modelling and optimization of different quality characteristics in electric discharge drilling of titanium alloy sheet" Material Today Proceedings, 21, 1680-1684. Available: https://doi.org/10.1016/j.matpr.2019.12.010

[13] A. Jain, A. K. Pandey, (2019), "Modeling and Optimizing of Different Quality Characteristics in Electrical Discharge Drilling Of Titanium Alloy (Grade-5) Sheet" Material Today Proceedings, 18, 182-191. Available: https://doi.org/10.1016/j.matpr.2019.06.292

[14] Riabi, H. K. B. Ayed, and L. A. Saidane, (2019). "A survey on blockchain based access control for internet of things," in 2019 15th International Wireless Communications Mobile Computing Conference (IWCMC), 2019, pp. 502–50. Available: https://ieeexplore.ieee.org/document/9718468

[15] A. Jain, A. K. Pandey, (2019), "Multiple Quality Optimizations in Electrical Discharge Drilling of Mild Steel Sheet" Material Today Proceedings, 8, 7252-7261. Available: https://doi.org/10.1016/j.matpr.2017.07.054

[16] V. Panwar, D.K. Sharma, K.V.P.Kumar, A. Jain & C. Thakar, (2021), "Experimental investigations and optimization of surface roughness in turning of EN 36 alloy steel using response surface methodology and genetic algorithm" Materials Today: Proceedings, Available: https://doi.org/10.1016/j.matpr.2021.03.642