Optimized Trust Management in Smart Buildings: A Blockchain-Based Approach Using ID3 Algorithm and IoT

SYED MOIDUDDIN RASHAD[1]
Lecturer, Computer Science Department, Science College, Northern Border University, Ar'ar, Saudi Arabia.

SYED MUTIUDDIN[2]
Lecturer, Computer Science Department, Science College, Northern Border University, Ar'ar, Saudi Arabia.

Abstract:

The study presents a comprehensive overview of the proposed solution for optimizing trust management in smart buildings through the integration of IoT with the ID3 algorithm and blockchain technology. Data about various areas in the building such as occupancy, temperature, and energy usage are accumulated through the utilization of IoT sensors that are distributed throughout the building. The ID3 algorithm is used eventually as a backbone for decisions that are built on analyzed sensor data and improving building operations. Trust management, with its multiple data sources and sensor readings, is evaluated by the model, while blockchain technology provides data integrity and security through decentralized control and governance. Smart contracts not only settle contracts but also give actions to be acted, bringing more to transaction efficiency. User privacy is maintained through the use of privacy-preserving techniques. A real-time monitoring system and optimization processes attain higher system efficiency the more time goes by. Adopting this comprehensive strategy ensures that smart buildings can achieve multi-faceted efforts in trust management, operations, and resilience to security lapses. As a consequence of this, they create safe, caring, and environmentally friendly surroundings.

Keywords: ***IoT, Blockchain, Smart Building, Trust Management, Cloud, ID3 Algorithm, Node***

I. INTRODUCTION

Nowadays, "trust management" is the set of tools and technologies applied to ensure the integrity, fairness, and security of the electronic mechanisms used by all the equipment and systems in the building. This method uses authentication and data integrity and keeps the networks between Internet of Things (IoT) devices and devices safe from unauthorized access, fraudulence, and damaging attacks. Security, likeness, identity detection and trust management are evolving due to Blockchain, IoT, ID3, and smart buildings becoming more secure and reliable. Decision Tree modelling through ID3 could search for aberrations and arrange data as best as possible. It can analyze and detect IoT network security issues and report them for fixing. Records in the Blockchain are peer-to-peer verified in that no consensual person is competent to hack data and deny access to information. All data transfers between devices are safe with IoT technology. It is written on a rock, which is immutable. It is an excellent reason because it is, without a doubt, everlasting [1]. The utmost benefit of Blockchain, IoT, and ID3 technology is reduced loss in trust management. The creation of a robust verification system across numerous domains, quick data fetching, and solid records of inspection can realize this.

The Internet has been increasingly integrated into the backbone of smart building systems that are based on IoT. While maintaining security and trustworthiness in smart construction networks might be difficult, an effective system for the management of the trust to mitigate the risk is introduced. There is a need for proper statistics studies to be undertaken to reveal whether or to what

level Blockchain is trustworthy in ensuring network security. Smart building 'management' could be enhanced by the ID3 algorithm 'through' Blockchain technology [2].

Believe computing is presented as an elective to current security strategies since this approach uncovers its flaws. This computation employs Bitcoin network belief and reputation data. The presented approach points to constructing an ecosystem that's secure and impenetrable to exploitation and conveys belief across all devices. This organization empowers secure conversations and transactions through membership confirmation and trust-based intuition. People believe appraisals can be calculated and coordinated using a hybrid strategy. Time-driven and event-driven strategies are utilized in this approach. This procedure ensures smart building IoT settings' reliability and credibility. The other potion discusses a piece of detailed information about the background, methodology of the presented system and potential results of implementing the system in the real-world scenario.

II. BACKGROUND

Trust is the most essential thing in the IoT ecosystem, considering the networking security issues and reliability problems that grow on the network of devices connected to each other. Grouping trust management strategies by the technology used and tools provides a view. It ensures that the complex issues of IoT cybersecurity are understood and dealt with appropriately. Architecture has many stages, headed by integration, network, and application. Trust management is also emphasized as having a significant role in the trustworthiness, security, and flawless performance of the IoT networks.

However, the dynamic phase of the process, which allows device identification, registration, secure data transmission, and access management, shows that trust is achieved. Local production at edge computing reduces the latency and improves the efficiency of the business. In edge computing, the storage and processing are closer to the user than in the Cloud [3]. Blockchain technology creates decentralized, transparent, and impenetrable ledgers. Such features make IoT-connected environments more reliable and secure. Researchers can get a clear idea of the advantages and drawbacks of each option by classifying the processes depending on such instruments.

Therefore, it is necessary to examine the ethical implications. Constant changes in the IoT settings make it difficult to maintain trust and meet moving security threats.

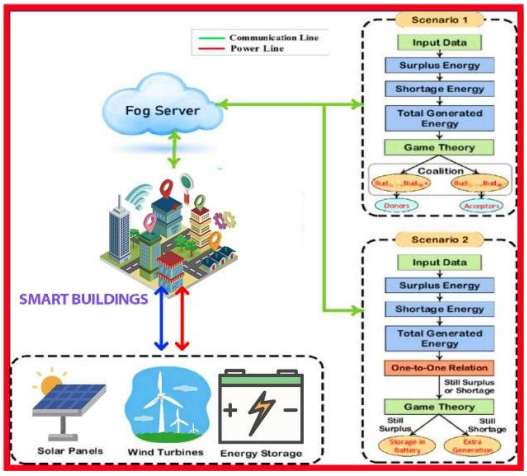

Fig. 1. Cloud-based Trust Management Systems in Smart Buildings [3]

Cloud Computing, as well as Edge Computing, constitute two novel ways to handle the vast amounts of data created by IoT devices. Computation at the frontier processes data locally, whereas cloud computing stores and analyses data on a massive scale. This reduces processing delays and improves system efficiency. These novel technologies are developed to manage the restricted resources of IoT devices to provide efficient and reliable data processing. The suggested system records interactions and transactions and collects trust data using a hybrid approach that combines time-based and event-based methods [4]. After collecting and consolidating this data, an unbiased administrator may assess it. This can depict the trust management to calculate a rating of trust for each device, indicating its network reliability. Blockchain technology, originally developed for Bitcoin, is ideal for IoT network security because of its decentralised and tamper-resistant design. This framework lets network members store and distribute reputation and confidence data. This approach helps devices distribute trust amongst neighbours, improving communication reliability and security.

Clustering algorithms and sophisticated networks may be used to increase algorithmic efficiency and examine the possible ramifications of employing the IoT to segment smart building networks. However, converting data into universal formats may improve IoT applications in many intelligent construction networks. In addition, indoor localization approaches like the Neighbour Relationship Method (LNM) have shown promise for accurate and fast localization in intelligent buildings. This allows IoT to be used in localization services, a real application [1]. Consensus algorithms are crucial to Blockchain technology because they maintain network integrity and foster trust. Different kinds of algorithms can be taken like Proof of Work (POW), Proof of Stake (POS), Practical Byzantine Fault Tolerance (PBFT), and round-robin algorithms. Each technique serves

a particular purpose to keep Blockchain ecosystems reliable and efficient.

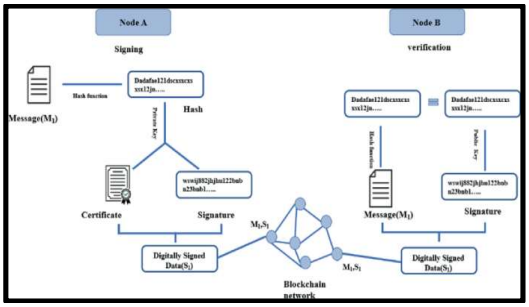

Fig. 2. Trust Management Model with IoT and Blockchain Technologies [6]

Building Information Modelling (BIM), IoT, and Blockchain are cutting-edge savvy building advances being examined. These innovations have different impacts, and each can be preferable in belief management. BIM is sometimes used throughout a building extend, from pre-construction to post-construction. It may moreover be connected to the IoT to improve building administration. Also, monitoring trust that developing projects can be optimized by improving HVAC technologies in independent structures utilizing IoT-driven explanatory management. Recreations can be made to optimize inside thermal comfort and energy use [5]. IoT components counting sensors, metering sheets, and control systems are significant for real-time building management. This diminishes energy utilization, maintaining comfort and proficiency.

III. METHODS

The smart buildings mobilizing IoT devices accompanied by the ID3 algorithm and Blockchain tech application unlock the mechanism of trust management, among others, leading to the most trustworthy and resilient system architecture. At its core, the method comprises three essential layers: a three-interlayer structure, which is the IoT Layer, Trust Layer, and Blockchain Layer. The IoT layer caters mainly to monitoring smart building systems that compactly collect crucial sensory data from the external environment. These tools, namely sensors, gauges, controllers, RFID (radio-frequency identification) devices, and computers are crafted to gather and save data, calibrate, or enter information for data acquisition and task accomplishment, respectively [6]. Furthermore, these modules carry additional features like mandatory licensing, which are customized to fit the current operating framework. These layers are the ones responsible for the collection of data and the subsequent communication of trust-related information, which depict devices on one side considering such items for assessment purposes and on the other acquiring such data from different devices.

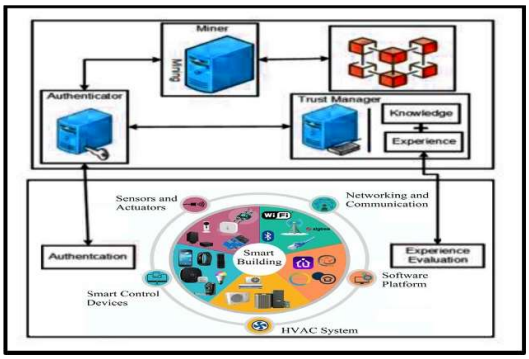

Fig. 3. Smart Building Operating IoT with Blockchain and ID3 Algorithm [2]

The Trust Layer comprises all attributes of the equipment. This hardware architecture provides security, workability, and reliability, and it is the base of the system planned to operate. The first phase takes place in the right part of the engineering trust layer, which is a place that safely stores scores of trusts and reputations and allows their use in a decentralized way. Accuracy parameters of a situation in visual form with the guidelines of nearby devices are instantaneous and, hence, involved in the complete network without common pattern changes. The exhibit includes the comfort of direct and indirect trust and the value of cooperation, which has essential knowledge and trustworthiness.

The Blockchain Layer is the core to guarantee that secured and authenticatable information is being accomplished through integrating Blockchain innovation. The integrity approvals of trust records and transaction information by miners are subject to the arrangement of detailed reviews, confirmations, and compromise mechanisms before being bundled into pieces and then included in the Blockchain record [7]. Multichain Blockchain technology is employed to make data secure, authorized by only selected personnel, and flexible authorization and delegation. The employed Blockchain technology provides the basis for transparency, honesty, confidentiality, and authorization in the processes of trust management.

$$T_{ab} = tri1 \times (T_{ab})^{(t-1)} + tri2 \times (T_{ab})^{(\Delta t)}$$

The equation Tab = tri1 × (Tab)(t − 1) + tri2 × (Tab)(Δt) calculates the trust value (Tab) of a device based on its previous trust value multiplied by tri1 and tri2 coefficients, representing the influence of past trust and changes over time (Δt). This iterative formula updates trust dynamically, considering both historical trust assessments and recent changes.

$$entropy(E)=(-p)/(p+n)\,[\log_2](p/(p+n)) - n/(p+n)\,[\log_2]\,(n/(p+n))$$

The entropy equation, entropy(E)=(−p)/(p + n) [log2](p/(p + n)) − n/(p + n) [log2] (n/(p + n)), measures uncertainty or disorder in a system with two possible outcomes, where p and n represent the frequencies of each outcome. It calculates the

entropy based on the probabilities of occurrence, using logarithmic functions to quantify the amount of information needed to describe the system's state. Machine learning techniques, of which the ID3 algorithm is a case in point, are the essential part of the approach for confident appropriate classification. The ID3 algorithm which is used after computing the trust values, will identify the maximum trust value out of all devices while the decision tree method will be used. Incorporation of this model accuracy trust assessment and consequently enhancement of the entire trust management process [8].

The application's new trust model creation and implementation criteria are specifically intended for functions to be carried out for accurate and proper efficacy. For this, the things that come under are a fast dynamic environment, device type diversity, and limited resources, which are considered. Trust measurements like single trust, distinct multi trust, and combined multi trust, which are subjective and objective trust properties, enable the factors to form the core of the trust adebs. This model of modelling means that issues of system trust can be distributed, time-driven, or even event-driven based on the behavior spelled through stations or the system's dynamism. Ultimately, combining IoT Devices, Machine Learning Algorithms, and Blockchain Technology results in a robust and complete Blockchain Management System for Smart Buildings [9]. So, the main task of this method is to create secure and reliable communication channels between IoT devices. It makes it possible to safeguard the integrity of key and identity data.

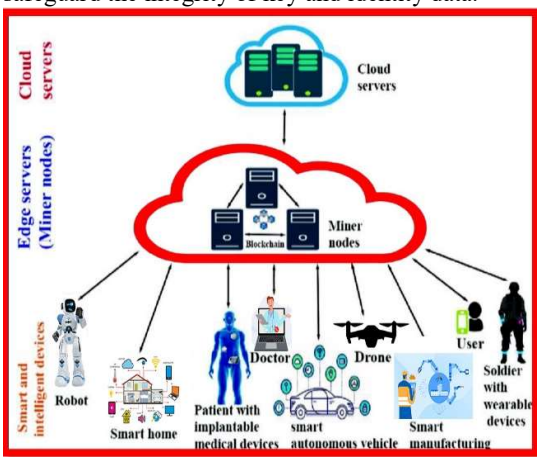

Fig. 4. Blockchain-based IoT Smart Building Architecture [19]

In addition to that, the suggested method puts the issue of trust model launching and design for successful functioning in an environment of diverse operations under the spotlight. The trust basis of the model demands a trustor and a trustee node as its backbone, with each trustor establishing trust while trustees are evaluated to ascertain their trustworthiness. Customers and vendors might happen to control the behaviour of the node in this case, while people of trust share their experiences about trading with others. The trust mode is flexible enough to consider direct and indirect ways of computation of trust. The essence is that these methods tap into the social environment from the observations and recommendations of other nodes, to make an accurate trust rating. Regarding the system architecture, the approach considers both centralization and decentralized approaches to trust management, as a function of the specific smart building network requirements. In the case of a centralized, one central node carries out the trust generation, creation, and spreading operations while on the other hand, in a decentralized system; each node independently takes care of its trust generation and transfer activities [10]. The technique's adaptability relieves it from being subject to the specification of each operational scenario or system complexity at any moment, thus improving the results and capabilities.

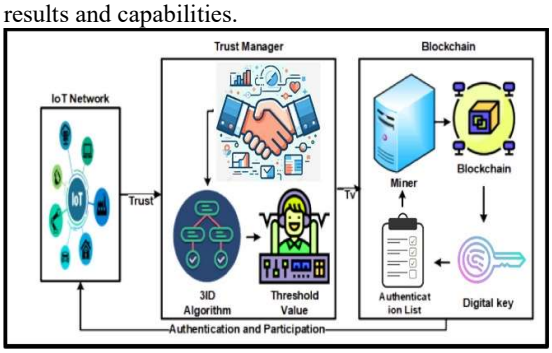

Fig. 5. A Conceptual Model of IoT with Numerous Interconnected Layers [1]

It also involves the innate aspect of trust, which needs to be updated forever due to the ever-changing cast of characters. Empirics, concrete things, can be supported since they follow people in the form of events or time. Nonetheless, the complex system may immanently dictate the whole process. This modification strategy involves integrating them to maintain the ability of the approach to monitor and adapt the assessment to the changing replay history purposes. The model also focuses on reliability and stability as the network infrastructure is exposed to threats and attacks to be highly used [11]. It has been observed that there are many service attacks, such as DoS attacks, data falsification plots, or the increment of scan activities, which, as a result, manage to exasperate the level of trust.

Combining IoT devices, Machine Learning Algorithms, and Blockchain innovation, the proposed strategy consists of a fair, orderly, and reliable standpoint for smart building belief management. This approach covers the plan considerations, standards, and clearing challenges and thus lays the foundation for creating brilliantly building ecosystems that fulfil the ever-changing demands of modern buildings.

IV. RESULTS AND DISCUSSION

NS3, a discrete network simulator, was used to realize the system. This has been achieved through the use of Ubuntu 18, which is now the standard in Scottish schools. 04., the prototype involved the smart environment building model with the IoT devices. The usage of gadgets has been ranged from a minimum of 10 or more than 30 gadgets. Each device had a randomly generated number from 1 to 10 to specify if it belonged to one of the ten official communities in the organizations and was not visible to others [12]. Agents in the hostile environment/area comprised 20% of the network. The main objective of this investigation was to assess system propriety against defamation, incremental voting, and tail attacks. The trustworthiness of the existing architecture was danced by tracing trust value shifts in response to unfavourable behaviours. Hence, the strategy has proved feasible as it minimizes cybersecurity attacks and increases system performance rate [13].

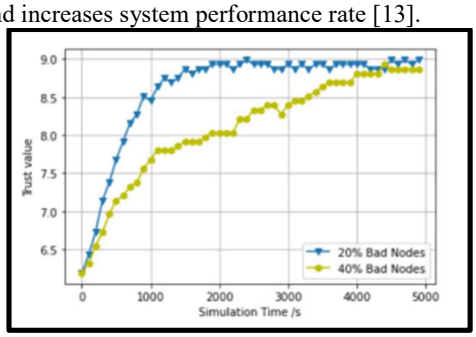

Fig. 6. Trust Implementation with Simulations of Nodes [1]

There were numerous key outcomes from the multichain of trust subsystem, reaction time, and energy consumption measurement statements. Through multichain, the data of trust information were kept securely and neatly in the IoT network, and communication was done smoothly. Cryptography, being the means of chaining transactions and storing the trust value, forms the essence of Blockchain. Concurrently, abrasion of an earlier examiner's creditworthiness ratings was made possible, thus making fraud detection and prevention an actuality. Confidence in the system has been strengthened and made more reliable once multichain was developed, and is now addressing defamation and vote tampering. The metric of response time demonstrated that the proposed system can handle Blockchain transactions and storage operations [14]. The demonstration of an effective system has been shown through its execution. An incremental relation is observed to be proportional to trust, for the average reaction time increased with the file stored in storage space. The ratings establish that the system is powerful enough to simultaneously grant and manage feelings of reliability. The solution proposed in the research on energy utilization was found to have consumed even lower amounts of energy than others. An upturn in energy consumption is achieved based on the capacity of the storage space surrounding the digital file.

Simulation parameter	Values
Simulator	NS 3.29
Simulator Run Time	2.5 hours
Nodes Distribution	Random
Total Number of nodes	30.....100
No. of compromise nodes	20% to 40%
Trust update time	500s
Starting trust value	1.0
Trust interval	0.....1
Poor witness node	21%
Malicious assisting nodes	11%
Type of traffic	Multimedia/messaging
Packet size	Constant

Fig. 7. Key Components of Evaluation of Trust Management Framework [1]

These analyses showed that multichain works for governing trust in sophisticated structures. The system's rapid response times and low energy consumption make it useful for IoT applications. Multichain's confidentiality and longevity have helped establish trust administration, which has improved smart construction safety. The technology demonstrated its ability to transport data consistently within the IoT platform via effective packet delivery [15]. Throughput measures the average rate of data packets transmitted from the starting node to the target node and back. The method has a high packet delivery rate, demonstrating its usefulness in smart building communication integrity and data transfer. This finding shows how trust management software supports data exchange amongst IoT gadgets and its stability and dependability. Overall, it shows how the system facilitates data transfer. After investigating the system's attack resistance, it was shown to reduce a broad spectrum of antagonistic behaviours [16]. The system detects and responds to bad-mouthing, endorsements wrapping, and on-off attacks by monitoring node trust and behaviour. The system's ability to identify and react to assaults makes this possible. The Blockchain-based design allowed monitoring and accountability, so hostile nodes could be detected and punished. This allowed for hostile action detection and punishment. The network's overall dependability and trustworthiness increased. Smart buildings are more secure and IoT data and connections are more accurate and reliable when they can resist attacks.

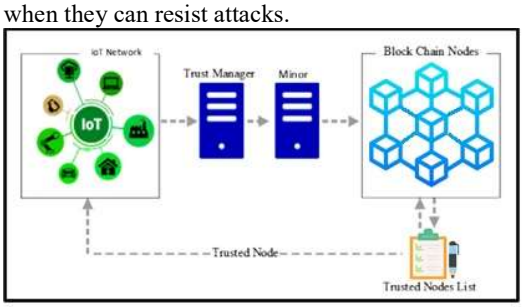

Fig. 8. Implementing Trust Model using IoT and Blockchain [1]

The study conducted a comparative analysis, revealing that the proposed system excels in secure messaging services regarding trust value, resilience, and performance criteria. Also, the approach was more efficient than previous methods since we always exceeded the existing trust value, reactive time, energy usage, and packet delivery. Thus, the comparative study demonstrates that the recommended approach is the best one when it comes to the issue of managing trust [17].

The results indicate that our suggested trust management method is better at delivering packets and resisting attacks and is a superior option to previously applied solutions. The execution of the strategy confirmed the fact that the proposed approach to more excellent governance on hybrid trust and the IoT ecosystems drives reliability. It demonstrates that the change in trust levels when the number of miscreant nodes differs could be a significant red flag of the resistance to attacks made [18]. Even in situations with considerable fraud, the system has proven workable. The trade-off analysis also intensely focused on overlooking the computer expenditure and its safety. The experiment results show that the Blockchain-based trust assessment is superior to non-Blockchain, which helps achieve accurate results.

V. CONCLUSION

The association of IoT device IDs and ID3 algorithms with Blockchain technologies can give you a smart solution that ensures calculated trustworthiness in smart buildings. It increases the power of all stakeholders to make data-based decisions, the level of security and the transparency of the building, and finally, these make the building environment more sustainable. The sensor analytics technology currently used can collect the complete legend from the sensor network. This data can be referred to as anything from the temperature and humidity levels to occupancy and energy usage patterns. Also, after that, it serves as a basis for the rest of the team members' decisions. Such data streams can be analyzed using the ID3 algorithm in real time. This algorithm can identify issues, make predictions, and optimize building operations. Also, the ID3 algorithm offers sensible solutions that managers can use to solve problems related to increasing efficiency and comfort in the working environment.

Furthermore, the application of Blockchain technology in the healthcare system ensures the integrity and security of information exchange among stakeholders, providing an additional layer of reassurance for healthcare professionals. Decentralization of a record made through Blockchain procedure is the primary constraint that guarantees an open, incorruptible, and steady database, making belief and accountability.

However, IoT devices will have the advantage of being mapped to a given gadget and their respective Blockchain recording, hence mitigating the risk of information altering and infiltration. Smart contracts also streamline devices' intelligence with any stakeholders, robotizing processes that account for the components of energy exchange, billing, and access control reasonably to ensure that the required rules and protocols are precise. Smart buildings are outlined in safer, more comfortable, and energy-efficient settings. These can be beneficial to workers by way of increasing productivity, satisfaction, and overall well-being. The trust, confidence, and transparency of blockchain transactions encourage the stakeholders and attract more partnerships and collaborations. In brief, IoT integrated with ID3 algorithm and blockchain technology is a new breakthrough in the history of smart buildings.

VI. ACKNOWLEDGEMENT:

The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA for funding this research work through the project number "**NBU-FFR-2024-1841-01".**

VII. CONFLICTS OF INTEREST:

No conflicts of interest.

REFERENCES

[1] F. Jeribi, R. Amin, M. Alhameed, and A. Tahir, "An efficient Trust Management Technique using ID3 Algorithm with Blockchain in Smart Buildings IoT," *IEEE Access*, vol. 4, pp. 1–15, 2022, doi: https://doi.org/10.1109/access.2022.3230944.

[2] M. Saeed, R. Amin, M. Aftab, and N. Ahmed, "Trust Management Technique Using Blockchain in Smart Building," *Engineering Proceedings*, vol. 20, no. 1, p. 24, 2022, doi: https://doi.org/10.3390/engproc2022020024.

[3] J. Zhao, H. Hu, F. Huang, Y. Guo, and L. Liao, "Authentication Technology in Internet of Things and Privacy Security Issues in Typical Application Scenarios," *Electronics*, vol. 12, no. 8, pp. 1812–1812, 2023, doi: https://doi.org/10.3390/electronics12081812.

[4] A. Konsta, A. Lafuente, and N. Dragoni, "A Survey of Trust Management for Internet of Things," Arxiv, arxiv.org, 2023. Accessed: 2024. [Online]. Available: https://arxiv.org/pdf/2211.01712.pdf

[5] K. Miličević, L. Omrčen, M. Kohler, and I. Lukić, "Trust Model Concept for IoT Blockchain Applications as Part of the Digital Transformation of Metrology," *Sensors*, vol. 22, no. 13, p. 4708, 2022, doi: https://doi.org/10.3390/s22134708.

[6] T. Zhao, E. Foo, and H. Tian, "A Lightweight Blockchain-Based Trust Management Framework for Access Control in IoT," *Smart sensors, measurement and instrumentation (Print)*, pp. 135–175, 2022, doi: https://doi.org/10.1007/978-3-031-08270-2_6.

[7] R. Jayanthi, S. Sundararajan, T. Alam, N. Garg, R. R. Singh, and M. Udhayamoorthi, "Building Trust Management using Blockchain Technology," *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, 2023, doi: https://doi.org/10.1109/icscds56580.2023.10104956.

[8] L. Bi, T. Muazu, and O. Samuel, "IoT: A Decentralized Trust Management System Using Blockchain-Empowered Federated Learning," *Sustainability*, vol. 15, no. 1, p. 374, 2022, doi: https://doi.org/10.3390/su15010374.

[9] Q. Arshad, W. Z. Khan, F. Azam, M. K. Khan, H. Yu, and Y. B. Zikria, "Blockchain-based decentralized trust management in IoT: systems, requirements and challenges," *Complex & Intelligent Systems*, vol. 9, pp. 6155–6176, 2023, doi: https://doi.org/10.1007/s40747-023-01058-8.

[10] R. Kumar and R. Sharma, "Leveraging blockchain for ensuring trust in IoT: A survey," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 8599–8622, 2022, doi: https://doi.org/10.1016/j.jksuci.2021.09.004.

[11] V. Dehalwar, M. L. Kolhe, S. Deoli, and M. K. Jhariya, "Blockchain-based trust management and authentication of devices in smart grid," *Cleaner Engineering and Technology*, vol. 8, p. 100481, 2022, doi: https://doi.org/10.1016/j.clet.2022.100481.

[12] R. Heidary, J. P. Rao, and O. Fischer, "Smart Buildings in the IoT Era – Necessity, Challenges, and Opportunities," *Springer eBooks*, pp. 1–21, 2023, doi: https://doi.org/10.1007/978-3-030-72322-4_115-1.

[13] F. Iqbal *et al.*, "Blockchain-Modeled Edge-Computing-Based Smart Home Monitoring System with Energy Usage Prediction," vol. 23, no. 11, pp. 5263–5263, 2023, doi: https://doi.org/10.3390/s23115263.

[14] G. Putra, V. Dedeoglu, S. Kanhere, and R. Jurdak, "Trust Management in Decentralized IoT Access Control System," arxiv, arxiv.org, 2020. Accessed: 2024. [Online]. Available: https://arxiv.org/pdf/1912.10247.pdf

[15] L. Fotia, F. C. Delicato, and G. Fortino, "Trust in Edge-based Internet of Things architectures: State of the Art and Research Challenges," *ACM Computing Surveys*, vol. 55, no. 9, pp. 1–34, 2022, doi: https://doi.org/10.1145/3558779.

[16] Y. Liu, C. Zhang, Y. Yan, X. Zhou, Z. Tian, and J. Zhang, "A Semi-centralized Trust Management Model Based on Blockchain for Data Exchange in IoT System," *IEEE Transactions on Services Computing*, vol. 16, pp. 858–871, 2022, doi: https://doi.org/10.1109/tsc.2022.3181668.

[17] M. Bampatsikos, I. Politis, V. Bolgouras, and C. Xenakis, "Multi-Attribute Decision Making-based Trust Score Calculation in Trust Management in IoT," *Proceedings of the 18th International Conference on Availability, Reliability and Security*, pp. 1–8, 2023, doi: https://doi.org/10.1145/3600160.3605074.

[18] R. Kumar and R. Sharma, "Managing Trust in IoT Using Permissioned Blockchain," *CRC Press eBooks*, pp. 127–149, 2022, doi: https://doi.org/10.1201/9781003283003-6.

[19] U. Khalil, O. A. Malik, O. W. Hong, and M. Uddin, "Leveraging a novel NFT-enabled blockchain architecture for the authentication of IoT assets in smart cities," *Scientific Reports*, vol. 13, no. 1, p. 19785, 2023, doi: https://doi.org/10.1038/s41598-023-45212-1.

Syed Moiduddin Rashad is a Lecturer in the Department of Computer Science at Northern Border University, Saudi Arabia. He holds dual Master's degrees in Computer Science and Engineering from Osmania University. His research interests include Machine Learning, Artificial Intelligence, Robotics, IoT, Blockchain, and Data Science. Widely recognized for his significant contributions, Rashad has authored numerous impactful papers in the Computer Science domain. His work bridges theoretical concepts with practical applications, enhancing both academic understanding and technological innovation. Through his dedication to education and research, he inspires the next generation of computer scientists and technologists.

Syed Mutiuddin, an enthusiastic Lecturer in the Department of Computer Science at Northern Border University, Kingdom of Saudi Arabia, is a dynamic researcher with a dual Masters degree. He holds a Masters in Technology in Electronics and Communication Engineering from Jawaharlal Nehru Technological University, Hyderabad, India. His academic interests encompass Robotics and AI, VLSI, Machine Learning, and Signal Processing. Widely recognized for his significant contributions, he has authored numerous papers that have significantly advanced the Electronics and Communication domain. With an unwavering dedication to academic excellence and a fervent commitment to technological advancement, Syed Mutiuddin remains at the forefront of pushing the boundaries of knowledge in his field.