Smart Blockchain based Protocol for IoT enabled Warehouse

Dr Sami Mahdi Elkofi

Computer Science Department, Prince Sattam bin Abdul-Aziz University

s.elkofi@psau.edu.sa

Abstract: The developments brought forth by the Internet of Things (IoT) are causing significant upheaval across a wide variety of business sectors. A variety of Internet of Things applications might prove beneficial to businesses in the logistics industry, particularly warehouses. These are only some of the many uses that may be improved with the use of this cutting-edge technology. Cloud-based apps and mobile cloud-based apps benefit from the IoT. We cannot rely on cloud-centric strategies since the world is moving toward more integrated solutions; instead, a decentralised strategy is required. End-to-end data warehouse design may be valuable for usage with the cloud-based Internet IoT technologies discussed in this article. Furthermore, the properties of edge computing allow for the creation of an efficient decentralised thing centric warehouse solution. Electronic systems will be able to function more autonomously if new protocols and better field devices, such as actuators and sensors, are installed. We will also look at non-functional characteristics like accessibility even when there is no internet connection, performance, response speed, reusability, security, and other equivalent characteristics. The Internet of Things is created by connecting a wide range of information-sensing devices to the internet and to one another. Despite the extensive usage of the Internet of Things, no linked devices may be utilised unless the integrity of the networks to which they are connected can be guaranteed (IoT). To address these concerns, a new protocol was developed that has been verified secure in both official and informal testing. Furthermore, this strategy has been shown to be effective. We were pleasantly delighted to see that our protocol exceeded the competitors in terms of both memory use and performance.

Keywords: Internet of Things, Blockchain, IoT Security, Thing Centric Warehouse, Smart Warehouse

1. Introduction

There has been a significant push in this direction, and by 2020, it is predicted that there will be 50–100 billion networked things [1]. To fully utilise and expand the capabilities of the unique environment, Rogers suggests a computing solution tailored to the domain [2]. He also talks about how ambient intelligence smart objects that have intelligence built, would anticipate needs and respond appropriately. Even though its major focus is on human beings, it is applicable to a broad variety of other topics as well. The way Roger thinks lend credence to the argument that context-sensitive intelligence is necessary anytime components specific to a certain region are used. Numerous applications have been created around this idea. IoT [3] has grown more ubiquitous in our daily lives. It collects data in real-time and makes it available for people to interact. Monitoring, connecting, and interacting with data is what this category is all about. The Internet of Things makes our lives easier and faster. Cargo VANs are widely regarded as one of the most promising IoT applications [4]. Another industry that has a direct influence on our everyday lives is healthcare, and the Internet of Things is being used in it. The appearance and feel of medical and healthcare facilities have changed dramatically because of the Internet of Things. If you have an internet-enabled health care system, wearable sensors

can help you collect data about patients and the environment they live in [5]. It is feasible to better people's lifestyles by having smart houses since these homes make people more comfortable, safer, and more productive. Furthermore, an IoT-based cloud system may assist the national government in better managing certain resources. By lowering the number of personnel required and utilising the management data provided by the cloud system, it is feasible to greatly improve resource utilisation. The cloud-based Internet of Things is a significant element in these benefits. It is likely that the introduction of this technology will result in improved data management by allowing authorised individuals to access normal data from diverse areas such as hospitals, houses, borders, and so on.

It has grown so normal that many individuals are unaware of the existence of the Internet of Things. As these devices become increasingly common, the importance of IoT security grows. Criminals have recently used IoT networks to carry out attacks. Because of these issues, the Internet of Things must be handled in terms of security to thrive. Because of the variety and complexity of these networks, deploying security measures for IoT networks is difficult. Furthermore, for the sake of data security, all data communications should be encrypted. As a result, communication between the two parties requires a shared session key. An authenticated key agreement (AKA) technique that is both safe and effective must be devised [6]. There are several AKA systems for the internet of things. It is built into their architecture [7] that an unauthorized user or an adversary with malicious intent may obtain a user's smart card and use it to compute the session key or guess passwords. As a result, we devised a new AKA approach to consider. A strategy has been developed that makes use of the fact that attackers are unlikely to acquire access to this information. We demonstrate that the suggested approach is safe against a wide range of assaults by employing Burrows-Abadi-Needham (BAN) logic [8]. Compared to the old strategy, the new one uses less memory and works better because of this.

Bitcoin was the first digital currency to use blockchain technology, and it is still the most popular one. Public blockchains and private blockchains are the two types of blockchain. As the name implies, a public blockchain was first suggested for distributed digital currency. In the framework for edge computing, it would assist in sustaining distributed transactions. In a warehouse, some deals would be made directly between the objects without the help of any middlemen [9]. Blockchain technology has various potential applications, including supply chain management, identity services, record keeping, and device control. There is a probability that distributed ledger technology will be utilised to secure business transactions one day [10]. Collaboration among users is required to ensure that the programme is constantly up to date. He then delves further into the philosophical underpinnings of economic notions like trade and money. The artwork displayed in the final paragraph is a piece of artwork displaying the conceptual modelling effort. This is how Parts 2 and 3 of this work are organised. Section 2 is devoted to related work ad section 3 shows the proposed model. Section 4 outlines the results and 5 shows conclusion. In this study, a smart warehouse solution built on blockchain technology is proposed, allowing IoT-enabled devices to communicate with one another.

2. Related Work

Participation in Related [11] Extracurricular Activities depending on how they are deployed, Internet of Things (IoT) systems can be classified as centralised, semi-centralized, or decentralized. When centralised systems are used, the physical resources of the data centre are taxed to the limit, forcing the use of extra processing capacity from the cloud or the back end.

There was only one point of failure since there was no direct link between peers. In an effort to find a solution to this problem, proxy copies and other solutions that needed a large amount of infrastructure were explored in an effort to find one. Nimbits and Thingwrox are only two of many possible examples. The XMPP protocol allows for the realisation of such an idea, Peer-to-peer communication is essential before semi-centralized systems may connect to a central server and become completely decentralised. Methods like ETSI M2M and SENSEI are examples of comparable approaches. In a decentralised system, users can talk to each other directly, so there is no need for a middleman. SensibleThing's platform and components in version 2.1 Decentralized systems such as SensibleThing and Filament are depicted in Figure 1.

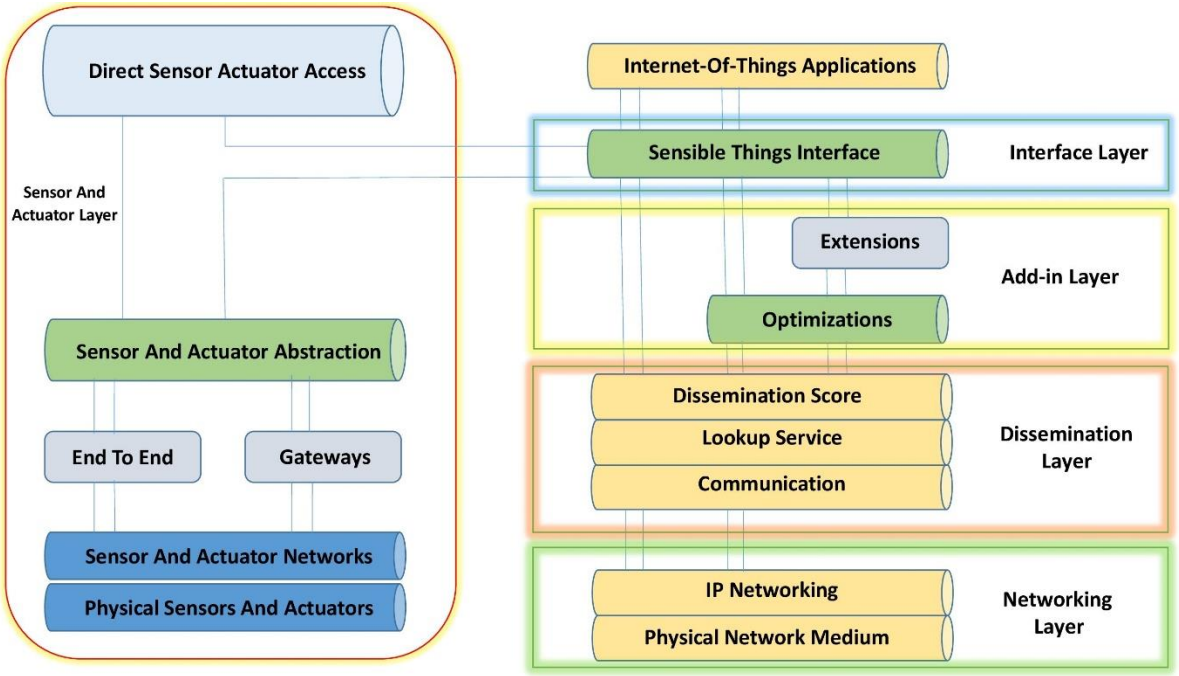

Figure 1. The architecture of The Sensible Thing illustrates how its components work together

Similar objectives for autonomous devices are shared by the Samsung Adept framework [12]. Distributed Context eXchange Protocol is the name of the protocol that they have developed (DCXP). A Universal Context Identifier is kept up to date by this application (UCI). Information is disseminated among all network participants at the dissemination Core layer. A lookup service to resolve UCI is present in this layer. IOT apps can access device capabilities through the Sensible Things interface. Blockchain transactions and automated "things" registration are both supported by Filament [13]. In Figure 2, a summary of the distributed stack is once again presented.

2.1 Blockchain Stack

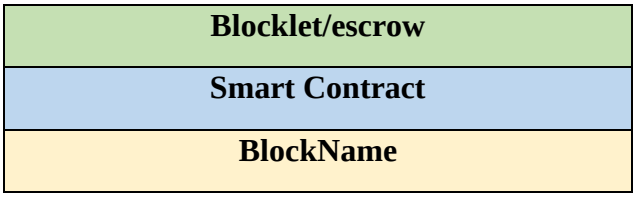

Figure 2. Filament stack

Blockname: To avoid using traditional DNS lookups, it resolves addresses using bitcoin. This makes distributed communication between devices possible. To create a hash string for device identification, telehash is used [14].

Blocklet: Blocklet is a transaction-supporting system built on the blockchain. Through an escrow system, it can also support microtransactions. This avoids the cost of using Bitcoin for microtransactions. Essentially, this is used for node-to-node transactions.

Smart Contract: A smart contract is a mechanism that may be used to govern and regulate the autonomous decision-making that occurs at the level of a device. Smart contracts are becoming increasingly important to the operations of businesses. In this paper, the feature of a filament is assumed to be the addition of a header and a cryptographic signature [15].

2.2 AWS IoT

Through the utilisation of a device gateway, the AWS Internet of Things solution generates server-side shadows of "things." To keep track of all the different kinds of gadgets, we employ a register. Device actuators act in response to any modification to the "things" shadow on the server side. A computer-based software system for inventory administration and tracking, according to the conclusions of researchers Atieh and Anas M. and their collaborators [16], might benefit from being expedited. An ERP-based solution that links to your field application can help you automate a process that you are responsible for. The automation process is impossible to carry out without this link. The idea of a dynamic scheduling system was conceived by Maschietto, Gabriela Naves, and a few other individuals to provide a solution to the challenges that are present in the current world. One of these issues is the need to go between two separate cranes. According to the term's definition, a heuristic is a specific type of computing method.

As stated by Nick Bennett, Alyahya, Qian Wang, and Bennett, RFID offers the capacity to automate a warehouse. Communication between multiple middleware systems, for example, must be reliable. This is only one of several rules that must be observed. Even if RFID makes it easier, maintaining a single record updated across the whole supply chain will be tough. Guido Follert, Nagel, Lars, and Moritz Roidl created an agent-based system for automated warehouse management that tackles the problem by dividing it down into its component pieces. as a result of his ability to perform well in a variety of contexts, including the field. One of the system's numerous drawbacks is the difficulty in keeping track of individual transactions when employing an agent-based system. The agent would be viewed as a separate entity from the rest of the company when it came to the actual job that needed to be done. Furthermore, it has a significant link with another system [17].

3. Proposed Model

"Thing-centered" This cutting-edge warehousing strategy is an amazing option that entirely tackles the problem. It will be possible to merge the judgments made by automated warehouse operations with those made by the corporate system using this technology. The utilisation of this strategy will directly result in the rapid feeding of information concerning the present status of the shop floor as well as its operating procedures and difficulties into the backend systems of the warehouse. One option to help alleviate some of the challenges that are now taking place is by making use of a "smart" warehouse that is built using IoT technology. This infrastructure

comprises sophisticated gate and forklift control systems, as well as IoT-enabled storage containers and loading bays. The present restrictions would be lifted as a result.

Figure 3 depicts the retention of a previously received cargo. An external source, such as a truck, would deliver a shipment to the warehouse. Following a visual inspection, the smart gate would update several parameters, such as weight and dimension, and transmit that information to business systems. The package is ready for pickup. If the message passed through the intelligent gate, it would be sent to all the smart items in the warehouse. Smart Forklifts and Smart Racks would all assess the communication to determine whether to participate in the transaction. The Blockchain transaction is taken part in by Smart Racks based on their contracts. The Blockchain framework will be used to build the consensus on rack assignment. Shipment information that must be brought to the rack will be broadcast by the designated Smart Rack. According to their contracts, it is up to the intelligent forklifts to study the message and decide whether to engage in the transaction. The distributed ledger technology known as blockchain will be used to build a consensus on the smart forklift option.

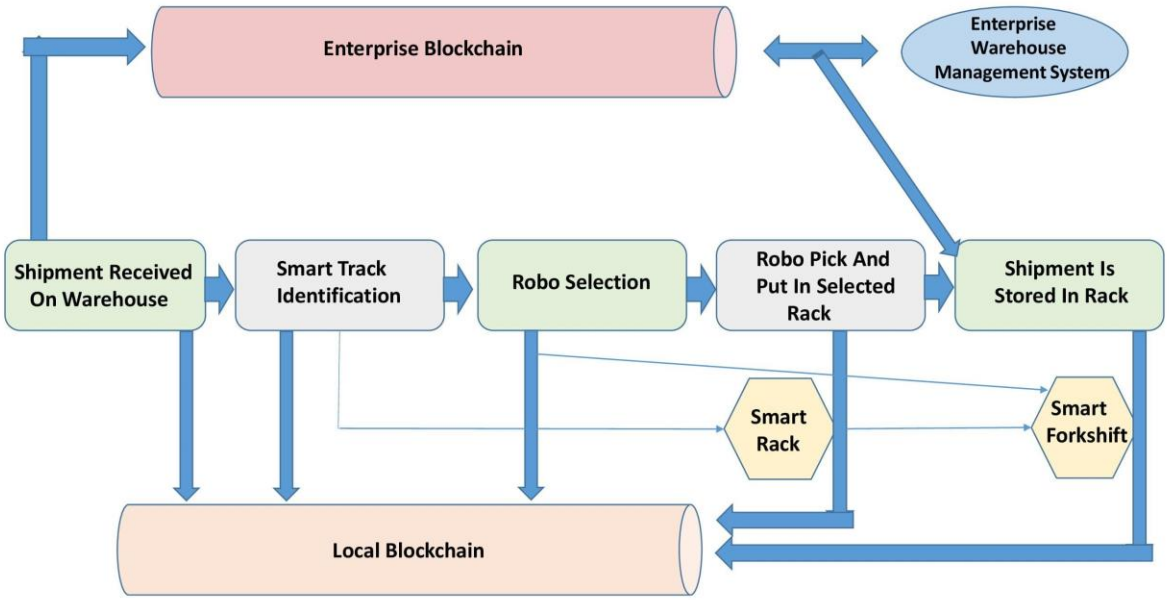

Figure 3. Taking Goods to and Keeping Them in Storage

In figure 4, we offer a model for utilising IOT and blockchain to make warehouses smart. A potential solution to Blockchain's constraints for the Internet of Devices is to employ decentralised technologies. This will help to improve service quality, increase communication, and ensure that organisational standards are met, among other things. To build a globally integrated economy, you will need a conceptual framework that ties together corporate software and field equipment.

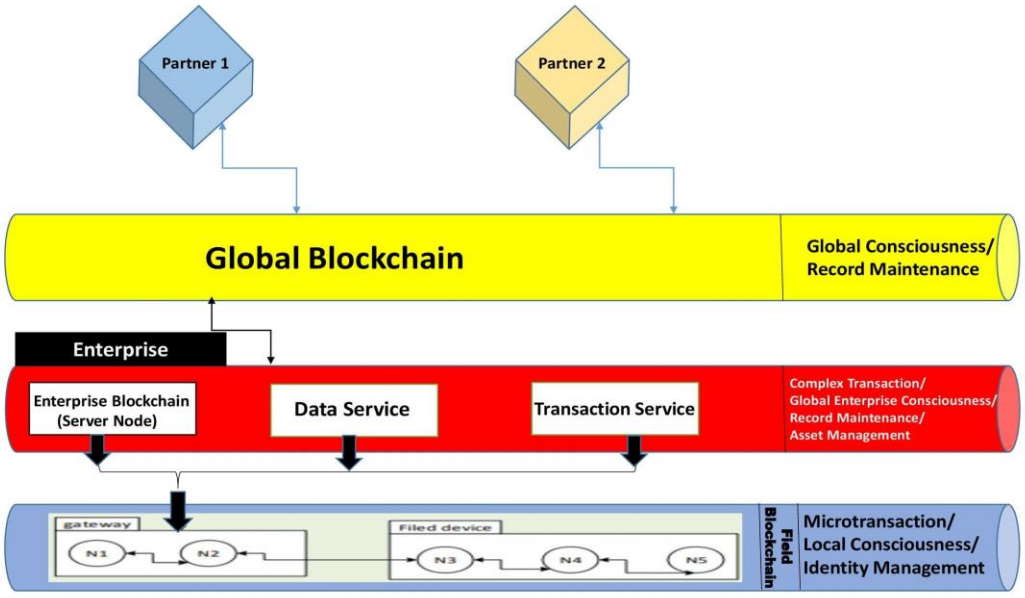

Figure 4. The Design of a Smart Warehouse

Smart Warehouse would be the name of the game if this design was ever put into action. A hierarchical blockchain, which looks to be more feasible, may fit the dispersed nature of blockchain within organizations, corporate computing, and partner engagement better[18-19]. This is possible because a hierarchical blockchain is more organized. As a result, the corporation has total control over how it manages its consumers' personal information. This strategy takes care of both the problem of being able to grow and the problem of having less time to react because of more awareness.

We'll go through the specifics of each phase of the process, as well as the overall picture, in this section of the conversation. The protocol's entire population is dominated by users and servers. The agreement covers functions such as registration and logging in, which are both necessary. Furthermore, there is the opportunity to change the password at any moment. The architecture of the proposed protocol is depicted in Figure 1. Because the user communicates with the entity, the user is the most crucial link in the chain. The server, on the other hand, represents the entity with whom the user connects.

3.1 Structural Elements

For a node to act as a smart item, it needs to have the ability to compute and a place to store information.

BlockName: Devices may now be uniquely identified at the device level, eliminating the need for a centralised system. If blockname was loaded locally, each device would have its own blockname. At the gateway level, where all devices are registered, there would be a mapping between the blockname of a device and the name of the organisation. This identical topic is being discussed at the business level.

Intelligent Contract: That's why this thing has a mind of its own. To accomplish this, the device makes use of a self-executing programme. This contract would be created to respond to

messages it receives and to construct context around those messages because of its replies. The section on use cases is a good place to see an example of this.

Blockchain: This is the most important element. This is the basic part of a local blockchain that helps people agree on something.

Gateway: Because of their gateway capabilities, these Smart Contracted Things can now communicate with a variety of different business processes. Their function is to connect the local blockchain to the company's main blockchain. The word "smart contract" would distinguish them from normal field equipment. Access to the server nodes that comprise an enterprise block chain can also be obtained through client-server protocols or low-level protocols. Gateways are used by both local and commercial blockchains, making them essential players in both sectors. For example, data and transaction services may be used to engage with and exchange data with corporate organisations. This is already conceivable. The data format is changed whenever a blockchain communicates with a corporate service.

Local Blockchain: In the hierarchy of blockchains, the local blockchain is at the bottom. Only this blockchain would be used by Smart Contract Things. The devices would use telehas/blockname to identify themselves [20]. The eligibility of "things" to take part in a Blockchain transaction would be determined by a "smart contract." The consensus would then be reached through a computation at the level of the blockchain [21]. Since all of these transactions are naturally private, external systems won't be able to see them.

Business Blockchain: Enterprise Blockchain involvement is required for transactions that call for enterprise level visibility, such as the transfer of products to a warehouse. The functionalities attained at this level are listed below. Records Maintenance: Two copies of the records would typically be always present[22-24]. One represents a record in the global block chain that can be tracked at the global level, and the other represents a record that can be tracked locally in a block chain. Managing assets, the health status of each "object" would be sent via each local blockchain. This can be used by enterprise-level data services to repair or spread defective equipment. There is no need for a separate system to monitor patients' health.

Send a failing device's status back to the business blockchain so that the proper action can be taken. Like this, sophisticated transactions can employ enterprise-level block chains. For instance, this hierarchical strategy speeds up transactions and consensus formation. Additionally, it separates responsibilities, which in turn makes cost-effective use of the idea of edge computing[25-28]. Even when the Smart Gateways are withdrawn from the network, there will be a path for communication between the Smart Contracted Internal Things and the Smart Gateways.

4. Experimental Result

We'd want to compare the Smart Warehouse with a range of different possibilities, such as central vs. decentralized storage, as per the paradigm that we've defined. A cloud connection is required for a centralized IoT platform to function. The flexibility and connection given by peer-to-peer networks is a critical component of decentralized systems. In our method, we will employ the least amount of monitoring and the least amount of access to centralized networks. As a result of this, each of these concerns will be resolved. The message is sent to everyone in the area through broadcast, and smart contracts are used to determine who is eligible to participate.

While IoT-enabled warehouse management systems may enable centralised decision-making, it is also likely that back-end solutions will be necessary to address the specialised demands of different areas to meet their expectations. Smart contracts can be used to make automated processes easier and to better understand what's going on with a device. Regardless of how blockchains are built, the technique employs a hierarchical approach to the chains. Because local transactions cannot be added to local blockchains, their influence on global block additions will be reduced. Commercially, it is feasible that the volume of local transactions may not warrant inclusion in the blockchain. As it turns out, this is far from the case. Using the technique given, incorporating the Internet of Things system into corporate operations will be done successfully and efficiently. On top of that, we'll create a gateway that can handle both regional and corporate chain transactions. To decrease chatter, communication with central systems should be limited to when essential. As a result, there will be less needless dialogue. Because of this, the back-end infrastructure will need much less processing, storage, and communication.

4.1 Investigations Examining the Relationship Between Performance and Safety

In this part, we look more closely at the proposed protocol's security and performance metrics. A typical method of performing security analysis is to compare the resistance of one proposed protocol to common attacks with the resistance of another proposed protocol. Another frequent method for finishing performance research is to evaluate the time and communication costs associated with various protocols. The next paragraphs will describe how this study compares to others that have used the same methodologies in the past. Some of the most common types of attacks are getting harder for older protocols to handle. The most common types of user impersonation attacks right now are A (Internal Data Security), B (Password Cracking), C (Replay Attack), D (Confidentiality), E (Session Data Security), and F (password guessing replay). Table 1 depicts the contradictory outcomes.

Table 1. Comparisons Of Secretive an Attack

Protocol	A	B	C	D	E	F
Lightweight Authentication Scheme	N	N	Y	Y	Y	Y
Authentication Scheme with Key Agreement	Y	Y	Y	Y	Y	N
Lightweight Dynamic Pseudonym Identity Based Authentication	Y	N	Y	Y	Y	Y
Authentication Scheme for Multi-Server Architecture	Y	Y	Y	Y	Y	N
Untraceable dynamic-identity-based remote user authentication scheme	N	N	N	Y	Y	N
An improved remote user authentication scheme with key agreement,"	N	Y	N	Y	Y	Y
Proposed Model	Y	Y	Y	Y	Y	Y

Because it is immune to all the security concerns outlined above, this protocol is more secure and trustworthy than other protocols of the same type. We compared it to a previous protocol to get a better feel of how this new protocol compares to the current alternatives. As a result, we used the same approaches and settings as Rana and her colleagues and relied on the data they provided to achieve more definitive conclusions [19] The findings indicate that, even while working in the same setting, different methods may take variable amounts of time to perform their tasks. The noncollision hash technique can be used 0.00014 milliseconds after a successful connection is established. The protocols will always ensure that the conversations take place in a risk-free environment. When security regulations are applied in a particular region, the procedure is streamlined. When an organisation is decentralised, it is more difficult to apply safety requirements. The introduction of numerous ways to address the problem has increased the problem's node-level complexity. The level of security enabled by blockchain technology is almost unparalleled [14]. Because their actions and actuations take place in their own local environs, Smart Things can regulate, localise, or remove concessions made on the back end. If gateway nodes oversaw producing explicit IDs, users would be able to register their identifiers with Smart Warehouse. For ID and Device Management to function successfully in a centralised system, gateways are required. You might want to use Smart Contracted Things if you have a local problem that doesn't need the attention of the whole company.

5. Conclusion

We believe that a hybrid strategy will help us to increase overall efficiency while maintaining continuity across all our sites. The IoT is causing significant upheaval across a wide variety of business sectors. The properties of edge computing allow for the creation of an efficient decentralised thing-centric warehouse solution. End-to-end data warehouse design may be valuable for usage with cloud-based Internet IoT technologies. The scalability of this proposal and other blockchain components will be evaluated to see if there are any problems that must be addressed before proceeding. The worldwide supply chain and other conditions may require changes to this method in the future. According to the study's findings, the Internet of Things remote protocol is not as secure as they promise. We compared our proposed protocol to others already in use and discovered that it takes less time and allows for more communication than the others. In comparison, the approach we presented is more adaptable and feasible for future studies.

Dataset

In this study, there is no dataset used.

Acknowledgment

The author would like to thank Prince Sattam bin Abdul-Aziz University-Saudi Arabia for supporting this study.

Conflicts of Interest

No potential conflict of interest was reported by the authors.

Funding Statement

No funding has been received.

References

1. Rogers, Y. (2006) Moving on from weiser's vision of calm computing: Engaging ubicomp experiences. In International conference on Ubiquitous computing (pp. 404-421). Springer, Berlin, Heidelberg.
2. Forsström, S., Kardeby, V., Österberg, P., & Jennehag, U. (2014). Challenges when realizing a fully distributed internet-of-things-how we created the sensiblethings platform. In The Ninth International Conference on Digital Telecommunications ICDT, 2014. (pp. 13-18).
3. Kozlik, P. (2015). Exploring Digital Currencies: Designing a peer-to-peer exchange with use of Blockchain.
4. Hompel, M., & Schmidt, T. (2006). Warehouse management: automation and organization of warehouse and order picking systems. Springer Science & Business Media.
5. Chen, M., Wan, J., & Li, F. (2012). Machine-tomachine communications: Architectures, standards and applications. Ksii transactions on internet & information systems, 6(2).
6. Presser, M., Barnaghi, P. M., Eurich, M., & Villalonga, C. (2009). The SENSEI project: Integrating the physical world with the digital world of the network of the future. IEEE Communications Magazine, 47(4), 1-4.
7. Bharimalla, P. K., Praharaj, S., & Dash, S. R. "ANN Based Block Chain Security Threat Mechanism", International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8(10), 2019.
8. Naseri, M., Abdolmaleky, M., Laref, A., Parandin, F., Celik, T., Farouk, A., ... & Jalalian, H. (2018). A new cryptography algorithm for quantum images. Optik, 171, 947-959.
9. Heidari, S., Abutalib, M. M., Alkhambashi, M., Farouk, A., & Naseri, M. (2019). A new general model for quantum image histogram (QIH). Quantum Information Processing, 18(6), 1-20.
10. Krishnamoorthi, R., Joshi, S., Almarzouki, H.Z., Shukla, P.K., Rizwan, A., Kalpana, C. and Tiwari, B., 2022. A Novel Diabetes Healthcare Disease Prediction Framework Using Machine Learning Techniques. Journal of Healthcare Engineering, 2022.
11. Ahmad, I., Serbaya, S.H., Rizwan, A. and Mehmood, M.S., 2021. spectroscopic analysis for harnessing the quality and potential of gemstones for small and medium-sized enterprises (SMEs). Journal of Spectroscopy, 2021.

12. Almarzouki, H.Z., Alsulami, H., Rizwan, A., Basingab, M.S., Bukhari, H. and Shabaz, M., 2021. An Internet of Medical Things-Based Model for Real-Time Monitoring and Averting Stroke Sensors. Journal of Healthcare Engineering, 2021.

13. R. Kashyap and A. Piersson, "Big Data Challenges and Solutions in the Medical Industries", Advances in Systems Analysis, Software Engineering, and High Performance Computing, pp. 1-24, 2018. Available: 10.4018/978-1-5225-3870-7.ch001 [Accessed 14 June 2022].

14. S. Kumari, M. K. Khan, and X. Li, "An improved remote user authentication scheme with key agreement," *Computers & Electrical Engineering*, vol. 40, no. 6, pp. 1997–2012, 2014.

15. Y. F. Chang, W. L. Tai, and H. C. Chang, "Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update," *International Journal of Communication Systems*, vol. 27, no. 11, pp. 3430–3440, 2014.

16. S. D. Kaul and A. K. Awasthi, "Security enhancement of an improved remote user authentication scheme with key agreement," *Wireless Personal Communications*, vol. 89, no. 2, pp. 621–637, 2016.

17. M. Rana, A. Shafiq, I. Altaf et al., "A secure and lightweight authentication scheme for next generation IoT infrastructure," *Computer Communications*, vol. 165, pp. 85–96, 2021.

18. M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 426, no. 1871, pp. 233–271, 1989.

19. D. Wang, D. He, P. Wang, and C. H. Chu, "Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 4, pp. 428–442, 2014.

20. R. Nair and A. Bhagat, "An Application of Big Data Analytics in Road Transportation", Advances in Systems Analysis, Software Engineering, and High Performance Computing, pp. 39-54, 2018. Available: 10.4018/978-1-5225-3870-7.ch003 [Accessed 14 June 2022].

21. R. Nair and A. Bhagat, "An Introduction to Clustering Algorithms in Big Data", Encyclopedia of Information Science and Technology, Fifth Edition, pp. 559-576, 2021. Available: 10.4018/978-1-7998-3479-3.ch040 [Accessed 14 June 2022].

22. R. Nair et al., "Blockchain-Based Decentralized Cloud Solutions for Data Transfer", Computational Intelligence and Neuroscience, vol. 2022, pp. 1-12, 2022. Available: 10.1155/2022/8209854 [Accessed 14 June 2022].

23. R. Kashyap, "Applications of Wireless Sensor Networks in Healthcare", Advances in Wireless Technologies and Telecommunication, pp. 8-40, 2020. Available: 10.4018/978-1-5225-9004-0.ch002 [Accessed 14 June 2022]..

24. R. Nair, S. Gupta, M. Soni, P. Kumar Shukla and G. Dhiman, "An approach to minimize the energy consumption during blockchain transaction", Materials Today: Proceedings, 2020. Available: 10.1016/j.matpr.2020.10.361 [Accessed 14 June 2022].

25. N. Waoo, R. Kashyap and A. Jaiswal, "DNA Nano array analysis using hierarchical quality threshold clustering," *2010 2nd IEEE International Conference on Information Management and Engineering*, 2010, pp. 81-85, doi: 10.1109/ICIME.2010.5477579.

26. R. Kashyap, "Big Data Analytics Challenges and Solutions", Big Data Analytics for Intelligent Healthcare Management, pp. 19-41, 2019. Available: 10.1016/b978-0-12-818146-1.00002-7 [Accessed 14 June 2022].

27. K. Xue, P. Hong, and C. Ma, "A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture," *Journal of Computer and System Sciences*, vol. 80, no. 1, pp. 195–206, 2014.

28. I.-C. Lin, M.-S. Hwang, and L.-H. Li, "A new remote user authentication scheme for multi-server architecture," *Future Generation Computer Systems*, vol. 19, no. 1, pp. 13–22, 2003.