Blockchain-Driven Software Solutions for Enhancing Trust and Security in IoT Environments

Sri Bhargav Krishna Adusumilli
Research Scholar
San Francisco Bay University Fremont, CA ,USA
bhargavkrishna.adusumilli@gmail.com

ABSTRACT:

The Internet of Things (IoT) aims to create a vast network with billions of things that can seamlessly create and exchange data, establishing intelligent interactions between people and objects around them. It is characterized with openness, heterogeneity, and dynamicity, which inevitably introduce severe security, privacy, and trust issues that hinder the widespread application of IoT. Blockchain technology has gained significant attention for its potential applications in the Internet of Things (IoT) realm. By combining blockchain with IoT, a new paradigm emerges that offers enhanced security, transparency, and trusting IoT networks. In the context of IoT, a blockchain serves as a decentralised and immutable ledger that records all transactions and interactions among connected devices. This decentralised nature eliminates the need for a central authority, ensuring that data exchanges and smart contract executions occur in a transparent and tamper-proof manner. Blockchain enables the creation of trusted ecosystems and facilitates direct peer-to-peer interactions between IoT devices. Through the use of smart contracts, devices can autonomously execute predefined actions based on predetermined conditions, eliminating the need for intermediaries and central control.

Keywords: IOT, Block chain, connected devices, high security.

I INTRODUCTION

The Internet of Things is a network of interconnected devices with the ability to process, compute and transmit data over a predefined network in an automated way and without human intervention [1]. The specter of this powerful technology could be traced in a broad range of applications such as smart home, smart energy management, smart mobility and Smart health to name but a few [2]. It is evident that IoT is transforming

and redesigning the Smart Cities environments by shaping new connections and interactions between citizens and devices in order to deliver better solutions. However, this smart technology raises new concerns and challenges related to data governance and storage facilities. In fact, smart devices, such as wearable sensors, capture massive amounts of data, including sensitive information about the citizen. Consequently, given the multitude of actors involved in a smart city environment with different interests for each, we need to define and control who can access which data, for what goal and how this sensitive information is stored and secured. Figure 1 shows the use of a centralized management of citizens' data collected by various smart devices and analyzed by a smart city data control centre. This kind of data management is vulnerable to data manipulation and disclosure as citizens need to have confidence in the entity that is storing their data assets [3].

Blockchain technology has emerged as a transformativesolution with the potential to revolutionise various industries, including the Internet of Things (IoT). By combining blockchain and IoT, a new paradigm emerges, offering enhanced security, transparency, and trust in IoT networks. This research paper aims to explore the integration of blockchain technology in IoT, its potential applications, benefits, and challenges, in order to shed light on its transformative impact. The Internet of Things (IoT) is a network of interconnected devices that communicate and share data seamlessly. However,the widespread adoption of IoT faces several challenges, particularly regarding security, privacy, and trust. Traditional centralised systems lack the necessary resilience to ensure data integrity and protect against unauthorised access and cyber threats. Blockchain technology, originally introduced as the underlying infrastructure for cryptocurrencies like Bitcoin, has gained attention as a potential solution for these challenges. The Blockchain serves as a decentralised and immutable ledger that records all transactions and interactions among connected devices. By incorporating blockchain into IoT, a trust less and more transparent environment can be created, empowering IoT networks with enhanced security and privacy features.

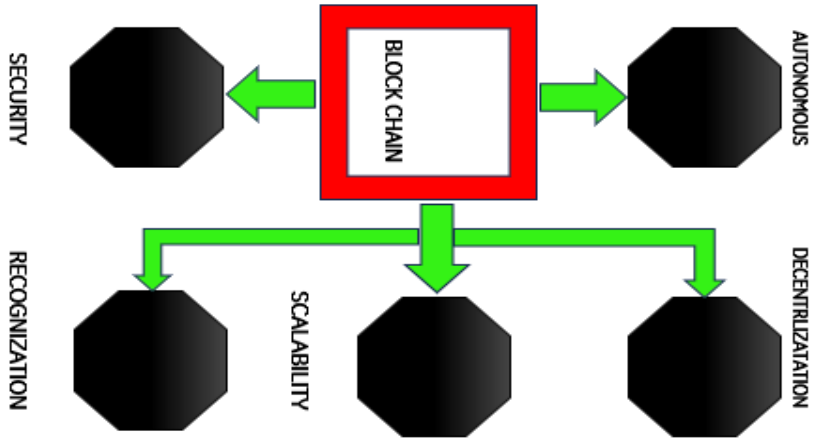

Fig.1. Model diagram

II SURVEY OF RESEARCH

In this [1], the authors provide a broad overview of the way blockchain technology might enhance the security and privacy-of IoT systems. and highlight the importance of decentralised consensus, control over access, and data trustworthiness in maintaining secure and private IoT networks. In addition to strengthening data integrity and reducing weaknesses in smart grid IoT systems, the authors in recommend using blockchain technology to enhance safety and confidentiality. In [2] , discuss how blockchain can be used to demonstrate the potential to address security and privacy issues in the setting of a smart home environment. For industrial IoT systems, the authors suggest a secure data-sharing framework that combines blockchain and attribute-based encryption. Theyemphasise how successful this strategy is. In IoT environments,they discuss how blockchain can provide transparent and immutable data storage, enabling reliable auditing and fostering trust among various stakeholders.

Recently, integrating the technology of blockchain in the context of smart city applications has attracted the attention of many researchers; however, a few of them note the importance of this technology in enhancing data privacy and security. “PrivySharing” a Blockchain-based framework for preserving privacy and security in smart cities, proposed by [3] is among the most important works. This system ensures the confidentiality of personal user data using Access Control Lists rules and smart contracts. Similarly, in another work [10] authors proposed a Blockchain-based

mechanism for sharing data in a smart city environment including non-trusted entities. The proposed approach allows an organization to take part in business actions by securely using data of other organization without accessing it.

Correspondingly, authors of [7] presented "SpeedyChain" a Blockchain-based system, which focuses on ensuring data integrity, non-repudiation and user privacy for smart real-time systems such as smart vehicle applications. It also uses a Blockchain architecture allowing fast data addition to the blocks. Nonetheless, this solution does not define different levels of data access control.

In [8], authors present "CitySense" a Blockchain-based approach to monitoring sensor data sharing in smart cities. According to the researchers, sensors produce useful data which must be available to citizens without modification. However, there are many security issues that need to be addressed. For instance, the issue of unsafe data sharing between a multitude of actors. Additionally, researchers in [9] propose a Blockchain-based framework to enable secure communications between actors in a smart city. Further, it ensures reliability, fault tolerance capability and scalability. Nevertheless, many technical aspects need further explanation, such as the consensus protocol and the Blockchain platform used in the smart city application.

III METHODOLOGY

The proposed network architecture is meant to make use of the cellular systems' capabilities and performance while providing an efficient and reliable security feature for IoT networks. To encrypt the multi-level structure, Evolutionary Adaptive Swarm Intelligent Sparrow Search is used. This research offers a framework to make it easier for IoT networked devices (objects and nodes) to be authenticated and authorized in a lightweight manner using blockchain technology. The entire cellular-enabled IoT network is divided into several levels by the suggested multi-level network paradigm.

The proposed approach aims to secure data sharing between different entities by combining data access control and audit mechanisms. Our solution is based on permission blockchains and smart contracts. It utilizes an enhanced Proof-of-Reputation consensus protocol as a hard security mechanism to secure data sharing in the smart cities environment. Contrary to past approaches that considered only the reputation property of a smart service provider, the proposed consensus model follows

a multidimensional approach taking into account other important criteria, such as its compliance with privacy laws and its compliance with citizens' preferences.

The goal is to calculate the overall trustworthiness of a smart service provider in order to:

1. Serve as the incentive for block publication and for keeping the ledger consensus on the Blockchain.
2. Be used to reward the service providers with high trustworthiness and punish those that may negatively affect system decisions.
3. Provide enough information so that a citizen can have an answer to the question if he can rely or not on a specific smart service for data sharing.
4. Be exploited to improve the reliability and trust in the provided smart services and increase the whole security of the smart system.

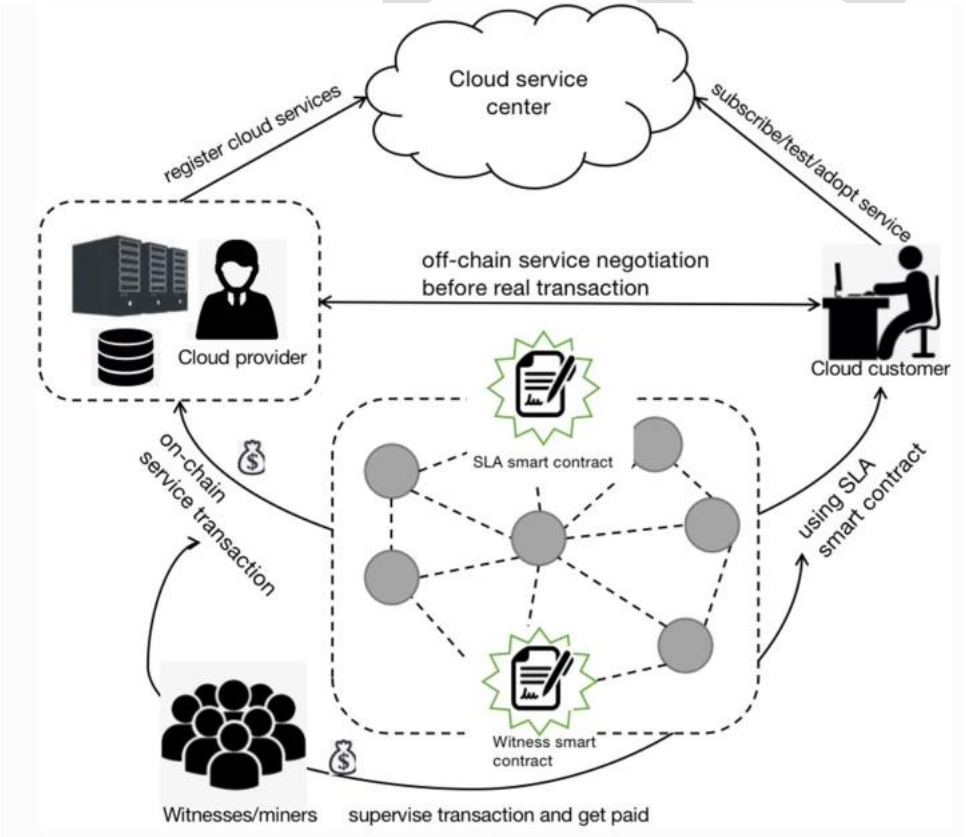

Fig.2.Proposed system model

Private blockchains: While so-called consortium blockchains are partially decentralized, private blockchains are completely centralized. We therefore use the term "permissioned". Indeed, they are defined as a private network managed by a

central body called the manager. The latter can modify the blockchain protocol as he wishes and is responsible for adding the blocks to the chain. The system is centralized and does not allow the link between the different participants. Although anyone can participate, access to this blockchain is restricted and requires the approval of the manager.

Participant layer: Comprises possible Blockchain network users. The participants/users access to the Blockchain network using a client application and a secure Web service.

Data layer: Instead of saving citizens' data over the network, we store encrypted data blocks in a cloud server which is connected to the Blockchain network. Once the data is stored on the storage server, it sends the hash of this data to the Blockchain network. The hash of the data is calculated using Merkle Tree. In this way, any modification in cloud data can be easily detected. We use the Diffle-Hellman Key exchange protocol to calculate the shared key that will be used for encryption/decryption operations with the AES symmetric algorithm. Control layer: this layer offers various APIs for different stakeholders. It is composed of the following components: Registration and Identity Verification Service (RIVS), Consensus nodes, Data Access Controller and Blockchains.

1. Registration and Identity Verification Service (RIVS): this module is responsible for X.509 certificate assignment and identity enrollment for different stakeholders. It retains the root certificate and generates a new certificate after the verification of the participant identity.

2. Consensus nodes: are nodes that participate in the implementation of the consensus algorithm so as to establish the ledger consistency. In the proposed architecture, all nodes are considered as consensus nodes. There exist two types of nodes: - Committing nodes: are nodes with the ability to execute smart contracts. However, they can just create transactions, validate and commit new blocks of transactions sent by the Miners nodes. We assume that every node in the proposed architecture is a committed node.

Miner nodes: In addition to the capabilities of committing nodes, Miners nodes are able to collect Transactions and package them into blocks and then broadcast those

blocks to the network. We assume that only service providers are eligible to be miner nodes.

3. Blockchains: In order to establish a secure environment for data sharing with authority control and audit ability, we use DataChain and LogChain as permissioned Blockchains. DataChain is mostly utilized for access control, and LogChain serves to provide a reliable and tamper-proof data access record. Both of them contain, in addition to the main Transactions (LogTx or DataTx), Trust Transactions in order to implement the consensus protocol based on trustworthiness.

4. Data Access Controller: is the module that interacts with the storage layer by using a smart contract-based access control.

CONCLUSION

The present paper examines a ground-breaking approach called the ”BC” and ”Internet of Things.” There are numerous opportunities and difficulties mentioned. In the following section, the kinds of services that are offered are also outlined.Since it could replace the existing web infrastructure with an entirely novel system in which every smart device is linked to other gadgets using a network of peers in current circumstances, this strategy may represent the Internet’s futuristic potential. It can speed up the process, save money,and instantly provide the appropriate data to the appropriate technology. Thus, it may be of significant assistance in the decades to come.

REFERANCES

[1] Bera A , “Insightful Internet of things statistics (Infographic),” White Paper. Retrieved from https://safeatlast.co/blog/iotstatistics/#gref

[2] Verma, R., Dhanda, N., Nagar, V, “ Towards a Secured IoT Communication: A Blockchain Implementation Through APIs,” In: Singh, P.K., Wierzchoń, S.T., Tanwar, S., Rodrigues, J.J.P.C., Ganzha, M. (eds) Proceedings of Third International Conference on Computing, Communications, and Cyber-Security. Lecture Notes in Networks and Systems, vol 421. Springer, Singapore. https://doi.org/10.1007/978-981-19-1142-2_53.

[3] Ali Haider Shamsan, Arman Rasool Faridi, “A Novel SDNFV IoT Architecture Leveraging Softwarization Technology Services to Alleviate IoT Network Resource

Restrictions, " International Journal of Engineering Trends and Technology, vol.70, no.2, pp. 1-10, 2022.

[4] Popkova, E. G., Ragulina, Y. V., & Bogoviz, A. V, "Fundamental differences of transition to industry 4.0 from previous industrial revolutions," In Industry 4.0: Industrial Revolution of the 21st Century , pp. 21-29, 2019. Springer, Cham.

[5] Walterbusch, M., Martens, B., & Teuteberg, F, "Evaluating cloud computing services from a total cost of ownership perspective," Management Research Review, 2013.

[6] Dahunsi, F. M., Idogun, J., & Olawumi, A, "Commercial Cloud Services for a Robust Mobile Application Backend Data Storage," Indonesian Journal of Computing, Engineering and Design (IJoCED), vol.3, no.1, pp.31-45, 2021.

[7] Lehner, W., & Sattler, K. U, "Database as a service (DBaaS)," In 2010 IEEE 26th International Conference on Data Engineering, (ICDE 2010) pp. 1216-1217, 2010. IEEE.

[8] Megha, C. R., Madhura, A., & Sneha, Y. S, "Cognitive computing and its applications," In 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), pp.1168-1172, 2017. IEEE.

[9] Preece, A., Cerutti, F., Braines, D., Chakraborty, S., & Srivastava, M, " Cognitive computing for coalition situational understanding," In 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) , pp. 1-6, 2017.EEE.

[10] Huang, K., Hussain, A., Wang, Q. F., & Zhang, R. (Eds.), " Deep learning: fundamentals, theory and applications," Vol. 2, 2019. Springer.

[11] Verma R., Dhanda N., Nagar V, "Security Concerns in IoT Systems and Its Blockchain Solutions," In: Tavares J.M.R.S., Dutta P., Dutta S., Samanta D. (eds) Cyber Intelligence and Information Retrieval. Lecture Notes in Networks and Systems, vol 291, 2022. Springer, Singapore. https://doi.org/10.1007/978-981-16-4284-5_42.

[12] Verma, R., Dhanda, N., Nagar, V, " Application of Truffle Suite in a Blockchain Environment, " In: Singh, P.K., Wierzchoń, S.T., Tanwar, S., Rodrigues, J.J.P.C.,

Ganzha, M. (eds) Proceedings of Third International Conference on Computing, Communications, and Cyber-Security. Lecture Notes in Networks and Systems, vol 421, 2023. Springer, Singapore. https://doi.org/10.1007/978-981-19- 1142-2_54.