Multidisciplinary Journal for Applied Research in Engineering and Technology (MJARET)

Vol. 1 Issue 5, December – 2021, Pages: 1-7

A PRODUCTIVE IBPRE MODEL FOR SECURE DATA SHARING IN BLOCKCHAIN TECHNOLOGY BASED IOT

DR K GURNADHA GUPTA

Associate Professor,Dept Of CSE

St.Martin's Engineering College, Dulapally, Kompally,

Secunderabad, Telangana 500014

MASTHAN RAO KALE **M.Tech., MIAENG**

Director ,Pooja Computer Education, Ongole,

Prakasam,Andhra Pradesh,India

Abstract: *Intelligent tailored services are necessary to fulfill the expectations of users. In order to provide a highly dependable service, additional information about the user's surroundings is required. In order to capture a vast quantity of data, the Internet of Things (IoT), which links multiple gadgets over the Internet, has been created. Although cloud computing is frequently utilized to effectively manage data, it has the potential to delay the transmission of data as well. In this work, we suggest a proxy re-encryption strategy to secure data sharing in cloud contexts. Data owners may outsource their encrypted data to the cloud using identity-based encryption, while proxy re-encryption construction will enable genuine user's access to the data. An edge device serves as a proxy server for computationally expensive tasks since IoT devices have limited resources. Using information-centric networking capabilities, we may effectively serve cached material in the proxy, hence enhancing service quality and efficiently using network traffic. We've also built our system on block chain, a revolutionary new technology that makes it possible to centralize the sharing of data. It reduces the load on centralized systems and allows for more precise management of data access. The security study and assessment of our scheme reveal the potential of our technique in protecting data confidentiality, integrity, and security.*

Keywords— *Block chain, data security, identity-based proxy re-encryption, information-centric network (ICN), Internet of Things (IoT).*

1. INTRODUCTION

One definition for the internet of things (IoT) is a network of interconnected devices that can exchange data without the need for human or computer-to-human interaction. These devices can include computers, mechanical and digital machines, objects, animals, and even people. They are all given unique identifiers (UIDs).

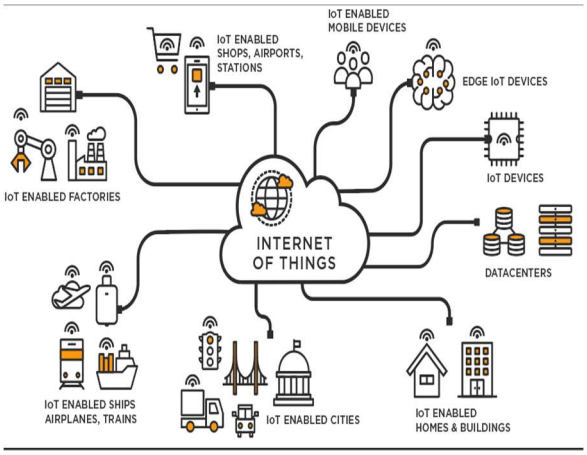

FIG 1: INTERNET OF THINGS

In fig 1 shows The Internet of Things presents vast opportunities in almost every industry. From remotely controlling crop irrigation to finding health issues in a person before they present to connected cars, IoT is exploding with opportunities and revenue.

Increasingly, firms in a number of sectors are utilizing IoT to run more effectively, better understand consumers to give superior customer care, improve decision-making and boost the value of the company.

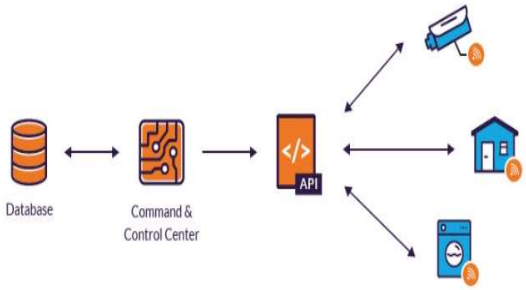

FIG 2: MANAGE OF INTERNET OF THINGS DEVICES

in fig 2 demonstrates Using a command and control centre (C&C), every IoT device is linked to a central management unit. Centers are responsible for software maintenance, configurations, firmware updates to patch flaws and vulnerabilities, as well as the provisioning and authentication of tasks, such as device registration. Communication between devices is possible through application programme interface (API) (API). Once a device's maker publishes its API, other devices or apps may use it to collect data and interact. Some APIs even provide control over devices. For example, a building management may utilise an API to remotely lock doors within a specific office.

In the field of "internet of things (IoT) security, the technology sector focuses on securing connected devices and networks (IoT). Incorporating an internet connection into a system of interconnected computers, machines, items, animals, and people is part of the Internet of Things. Each object has a unique set of identifiers and the ability to autonomously transfer data via a network. As long as they aren't sufficiently safeguarded, gadgets that link to the internet face a host of serious dangers"[8].

Due to many prominent occurrences where a common IoT device was abused to access and attack the larger network, there has been increased interest in IoT safety. The security of networks with IoT devices connected is critical. IoT security comprises a large range of methods, strategies, protocols and actions that strive to limit the developing IoT hazards of current organizations.

The Internet of Things (IoT) connects people, places, and things, opening up new opportunities for value creation and monetization for everyone involved. IoT devices are loaded with sophisticated electronics, sensors, and actuators that wirelessly communicate data to the IoT network. The analytical capabilities of the IoT harness this data to translate insights into action, transforming business processes and leading to new ways of working. However, a number of issues relating to technology and security remain.

IoT's widespread adoption has been hampered by concerns about security. "Distributed Denial of Service (DDoS) attacks are particularly effective against Internet of Things (IoT) devices because of common security flaws. Attacks using distributed denial-of-service (DDoS) cause the targeted system to be rendered unusable for its users due to the overwhelming volume of simultaneous data demands coming from several compromised computers. Disruption of companies and individuals has been caused by many DDoS attacks in the recent past Unsecured IoT devices give an easy target for cyber-criminals to exploit the weak security safeguards to hack them into beginning DDoS attacks" [4].

Another challenge with contemporary "IoT networks are one of scalability. As the number of devices connected through an IoT network develops, conventional centralized methods to authenticate, authorize and connect multiple nodes in a network will develop into a bottleneck. Servers that can handle the massive amount of data being sent will be needed, and

the whole network may fall down if one of those servers fails." [5].

According to Gartner's "Forecast, Internet of Things endpoints are anticipated to expand at a compound annual growth rate of 32 per cent from 2016 through 2021, reaching an installed base of 25.1 billion devices. With IoT devices projected to be such a crucial part of our daily lives in the future years, it is essential that organizations participate in solving the aforementioned security and scalability challenges" [6].

Another game-changing technology, block chain, or distributed ledger technology (DLT), has the potential to assist with IoT security and scalability challenges. Because of its unique capabilities and advantages, block chain is referred regarded as an "information game changer." It is impossible to amend or erase transactions after they have been recorded in a distributed digital ledger on the Internet and shared among the system participants in a block chain system. Using it, a group of individuals may gather and share data. Within this community, chosen members keep their own copy of the ledger, and new transactions must be vetted collectively via a consensus process before being allowed to the ledger. Please check Deloitte's prior report The Block chain (R) evolution for more information on block chain technology.

"The amazing qualities of block chain technology that is useful in traceability, security, transparency. A block chain-based system is installed to give a secure decentralized tracking mechanism. System design depends on the ethereal block chain and smart contracts to reduce the need for third-party system administration. The programmed consists of a smart contract for Ethereum, which incorporates the operations of the supply chain, in addition, it has offered the ability to save and retrieve records from the blockchain ledger, which makes it simple to monitor the product and verify that the data cannot be modified. Our local blockchain (created by Ganache) is linked to the Ethereum wallet through MetaMask to build a transaction bridge. This includes the arranging of transactions or of medicines. Solidity's programming code is fundamentally contained in contracts that are a contract in Solidity is a collection of code and associated data that exist at a single address on the ethereum blockchain. A contract indicates that is typically a core element of constructing an app on ethereum" [7].

Blockchain and IoT are both new technologies with immense promise, but are missing mainstream acceptance owing to technical and security issues. Several businesses in the industry are already working on use cases integrating the two technologies, since combined they provide a method to limit the security and concomitant commercial risks.

2 RELATED WORK

A proxy may re-encrypt an encryption computed using Alice's public key into one suited for Bob. Alice may use this method to temporarily relay encrypted messages to Bob without giving him her secret key. It doesn't know Alice or Bob's secret keys and doesn't learn the plaintext during the conversion, which makes proxy re-encryption schemes untrustworthy. The proxy and Bob are not allowed to interact; therefore it is assumed that at least one of them is honest, or that their collusion is blocked or detected. Several public-key encryption proxy re-encryption protocol ideas exist. With Identity-Based Encryption (IBE), senders encrypt messages using the recipient's identity (a string) as the public key. By giving Alice's email address, Charles could encrypt a message. In addition to overcoming key distribution concerns, identity-based encryption has enabled the creation of innovative cryptographic protocols such as secret handshakes, public-key searchable encryption (CCA2), and digital signatures. The Bone-Franklin technique works well and is widely used." [2].

A proxy may transform an encryption computed under Alice's identity to Bob's using our identity-based proxy re-encryption (IB-PRE) schemes. The proxy employs proxy keys, sometimes called re-encryption keys, to finish the translation without understanding the plaintext. The proxy keys also don't reveal Alice and Bob's secret 1keys. Utilize existing Boneh-Franklin IBE installations, secrets and settings.

A Private Key Generator (PKG) is a trusted source of keys for Identity-Based Encryption (IBE) (PKG). As a consequence, the PKG may possibly produce proxy keys. The Private Key Generator is not involved in our schemes. Instead, individual users grant their own decryption rights. There are theoretical and practical reasons for this. However, having the PKG produce proxy keys is plainly unacceptable from a practical standpoint. Forcing the PKG to remain online and available during the creation of proxy keys (other than IBE keys) and creating (potentially unwanted) decryption privileges in specific programmers.

3.ROPOSAL WORK

Safe data confidentiality and fine-grained data accessibility are achieved via the use of our access control system. This will also guarantee data owners' ultimate control over their data.

Our system architecture in Fig. 3 presents a blockchain-based PRE technique to data sharing. "The

edge devices function as proxy nodes and provide re-encryption services to the permitted user(s) (s) (s). When the data is cached at the edge of the network, the edge devices give services to users with high availability and performance. The data owner provides the re-encryption key, the CSP provides the ciphertext, and the CSP transforms the ciphertext into the user's identity. It is an honest-but-curious entity" [1].

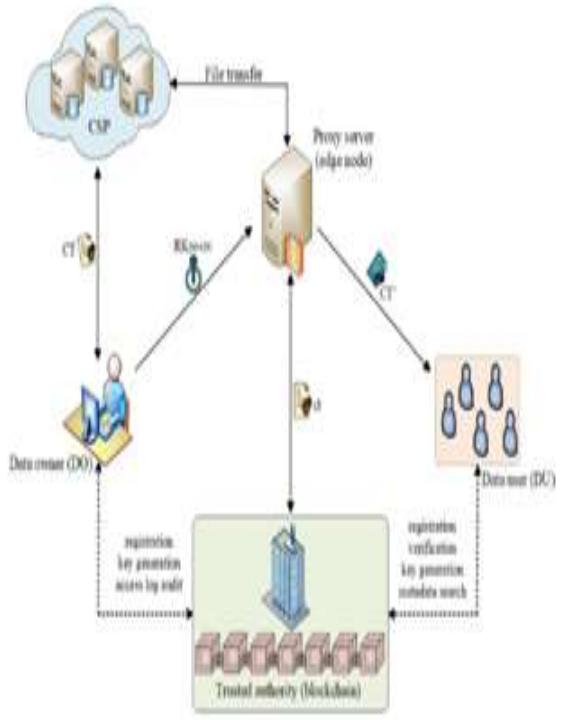

Fig. 3. Data-sharing system model.

The block header's components are crucial in constructing an accurate and trustworthy header. The hash of the preceding block is a 32-bit string that protects the chain by being connected to the previous or parent block. Miners apply a 4-b long nonce to produce numerous permutations and also build a valid hash in the sequence. Everyone can view the encoded record of an event owing to the timestamp. It is 4-b long and generally gives the date and time of block creation. Hashed transactions are stored within hashed transactions as part of the Merkle root. The target difficulty is used to modify how challenging it is for miners to solve the block, while the version number maintains track of modifications and updates. Each of them has a byte length of four. A total of 80 bytes make up the header. Figure 4 explains how to put together a block.

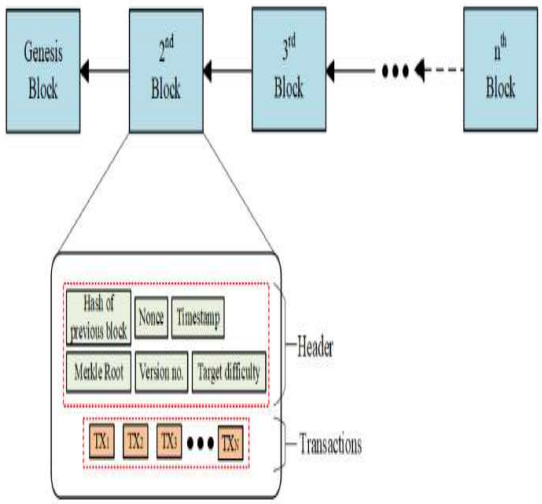

Fig. 4. Block structure

In dynamic IoT environments, centralized data services result in high bandwidth consumption and server load and are, therefore, not scalable to satisfy the rising demands of IoT systems. A consortium blockchain is employed thanks of its applicability to access control and privacy protection. Data may only be accessed by those who have been given authorization. Data owners can appropriately manage their data and audit records. Consortium block chains provide a great degree of security. IoT security challenges that are solved by the blockchain network include validating the identity of the connected users or devices, their account information, and also preventing cached data from being exploited.Because edge devices have large processing capabilities and storage, they act as proxy servers to deliver re-encryption services and other computations for the resource-constrained IoT devices. It is, consequently, straightforward to cache data at these edge nodes. Retrieving data through high-speed networks, the user

may make re-quests for data access, hence creating a smooth user experience. Devices at the edge, as well as other stakeholders, must have different identities because of edge networks' dynamic and movable natures. The ID of all entities in the network is represented by the tuple (id, kpu, kpr, rl) (id, kpu, kpr, rl) (id, kpu, kpr, rl). The public key kpu's cryptographic hash is represented by id, hence id = hash (kpu) (kpu). The private key is represented by kpr, while the function of the entity is represented by rl. The edge devices themselves could be data users, in addition to the roles performed by the data owner and user. To commence a transaction, each party's identity must be verified and authenticated. Attempts at verification will be refused, and the connection will be turned off. A static cryptographic problem termed S/Kademlia is used to produce public and private keys that can't be compromised by a Sybil attack. The public key is used to sign communications (transactions) in order to verify their legitimacy.

CONCLUSION

Data sharing is a well-known usage of the Internet of Things. A secure identity-based PRE data-sharing mechanism for cloud computing is presented. Owners of encrypted data may store it in the cloud and distribute it quickly with qualified users using IBPRE technology. Due to resource constraints, an edge device performs complex computations. The method also makes advantage of ICN's ability to distribute cached data properly, improving service quality and network resource efficiency. Then we provide a blockchain-based system paradigm for customizing encryption privileges. Fine-grained access control may allow data owners to maintain reasonable privacy. The proposed model's study and results show how efficient it is compared to previous systems.

REFERENCES

1. K. O. -B. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia and J. Gao, "A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain," in IEEE Systems Journal, doi: 10.1109/JSYST.2021.3076759.
2. Green, M. and Ateniese, G., 2007, June. Identity-based proxy re-encryption. In International Conference on Applied Cryptography and Network Security (pp. 288-306). Springer, Berlin, Heidelberg.
3. Hassanien, A.E., 2021. Digital Transformation and Emerging Technologies for Fighting COVID-19 Pandemic: Innovative Approaches (Vol. 322). Springer Nature.
4. Raj, P., 2021. Chapter Eighteen-Industrial use cases at the cusp of the IoT and blockchain paradigms. Adv. Comput., 121, pp.355-385.
5. Janardhana Swamy G.B., Janardhana D.R., Vijay C.P., Ravi V. (2022) Blockchain-Enabled IoT Integrated Autonomous Sewage Management System. In: Gururaj H.L., Ravi Kumar V., Goundar S., Elngar A.A., Swathi B.H. (eds) Convergence of Internet of Things and Blockchain Technologies. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-76216-2_3
6. Kamble N., Gala R., Vijayaraghavan R., Shukla E., Patel D. (2021) Using Blockchain in Autonomous Vehicles. In: Maleh Y., Baddi Y., Alazab M., Tawalbeh L., Romdhani I. (eds) Artificial Intelligence and Blockchain for Future Cybersecurity Applications. Studies in Big Data, vol 90. Springer, Cham.

https://doi.org/10.1007/978-3-030-74575-2_15

7. Mrs. P. Vinayasree, Dr. K Gurnadha Gupta."TRACKING OF MEDICINES OVER BLOCKCHAIN" PAIDEUMA JOURNAL, Vol XIV Issue 7 2021.
8. Anantharam, B. and Guptha, G., 2016. Security Issues in Various Cloud Computing: Solution and Occur-Rent Solutions. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN, pp.2456-3307.