An Efficient Blockchain Based Privacy Preserving Algorithm for IOT Applications

Sangeeta Gupta, Shaik Nafisa

Department of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology, Gandipet, Hyderabad

Corresponding author: Shaik Nafisa, Email: snafisa99@gmail.com

One of the most fundamental criteria of any cloud-based platforms, in particular, must protect the privacy and integrity of its users at all times, mainly when virtualized, is to maintain privacy and integrity. Block chain is a relatively new technology that has become a prominent factor in securing cloud-based services. Blockchain has late surfaced promising answer for cloud cluster combination and exchange security. Blockchain has lately emerged as a potential platform for cloud transaction security, and information and application code access. The principle objective to integrate blockchain innovation is to encode different and monstrous information, and then to decrypt the data once it has been transformed into hash values. In addition, more robust and superior hash algorithms, such as SHA-256 and SHA-384, are now accessible. To prevent data from being attacked, we are using the SHA512 method, followed by the RSA algorithm to recover the original data. Subsequently, as far as the time it takes to figure a solitary hash, we consider SHA512 to be more secure and reliable. As a result, in the proposed work, we are using enhanced SHA512 and RSA to increase reliability.

Keywords: Blockchain, SHA, Encryption,Security, Decryption.

2023. In Saroj Hiranwal & Garima Mathur (eds.), *Artificial Intelligence and Communication Technologies*, 857–862. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-955020-5-9-80

1. Introduction

The Internet of Things (IoT) is an adaptive self-configuration network that enables communication and interaction between physical things, turning them from blind to smart. As a result of its tremendous impact on our daily lives, the IoT has recently gained attention [4]. We may expect a wide range of IoT applications across a wide range of industries to have a significant impact on our lives [3]. This technology can be used in a variety of ways [1][2], including in terms of healthcare, transportation, and home automation. Service Providers are asked to provide the services that Cloud users need (CSP). Third parties, such as CSPs, offer cloud storage services to their clients. It is predicted that other third-party service providers, such as TPAs and Attribute Authority (AA), would have cloud protection capabilities [1]. Cloud-based enterprises and institutions rely heavily on security and trust, as we all know. Users of the cloud have no idea with whom they are exchanging communications or information. When it comes to transparency, it's critical since cloud users don't know who their data users are or how their data moves across the cloud. Cloud users can take advantage of blockchain technology, which is always changing and innovative, to strengthen trust, maximise decentralised blockchain efficiency, and safeguard data when using cloud services [2][3]. Security in Blockchain is superior to that in centralised databases.

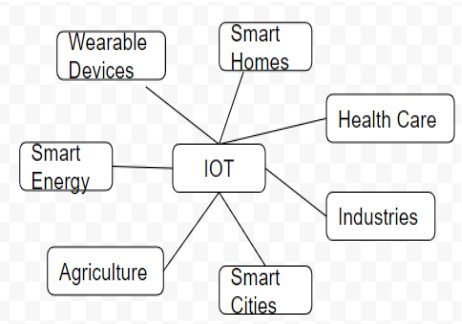

Fig 1: Applications of IoT

Using a blockchain, transactions can be tracked and manipulated can be prevented. Peer-to-peer networks are widely used to run blockchains, which are meant to prevent arbitrary modification. Blockchain may provide the same level of security as centralised database storage. Losses and attacks on data storage can be avoided from a management perspective. Openness and data integrity are two of the benefits of using blockchain technology in a data-sharing environment. A number of industries are expected to benefit from this technology, including the financial sector and the Internet of Things (IoT). There has been a lot of discussion about cloud security and safety in terms of the primary security elements. Businesses who develop and manage blockchain software can use the term "blockchain-as-a-service," which refers to distributed storage and organization for such companies [4]. A blockchain-based app's backend is handled by Baas, which functions similarly to a web host. Changing, hacking, or scamming the system is nearly impossible with a blockchain-based data management system. Decrypted and replicated digital data processing ledgers, known as blockchains, can be found on any computer network [5]. IoT can benefit a wide range of businesses including those in the hardware and serviceindustries as well as those that create software for these businesses (IoT).

In recent years, organisations and people have increasingly turned to cloud computing and big data technology to store and process their data remotely. In the cloud, personal medical information and corporate internal data are two types of sensitive data that is often kept. Ciphertext is used to protect both data and user privacy when data is stored on a cloud server. Encryption can be viewed as a safety net for controlling access to data. But how to control access to encrypted data is a significant concern. Crypt text-policy attribute-based encryption (CP-ABE) was first developed in 2007 by Bethencourt. In CP-ABE mode, ciphertexts and private keys are linked to access policies and attribute sets. Using the provided ciphertext, you can only decode it if the user's attribute set complies with the data owner's policy for data access. The data user receives the matching key from the attribute authority centre. The data owner has the authority to set restrictions on who gets access to the data. The entire system is at risk because of the corruption of the government's top officials. Therefore, a decentralised access control system is necessary to eliminate the threat posed by an authoritative, centrally-controlled authority. In recent years, a number of people have looked into blockchain-based access control approaches, but most of them have come up with a framework

or concept for such schemes. No single solution exists for integrating blockchain technology with access control technology. As a result, there is still a great deal of progress that can and should be made. Blockchain-based studies into decentralised access control are therefore incredibly beneficial. Data that must be stored on the blockchain network while still being monitored and tracked can be encrypted using ciphertext policy characteristics and the Ethereum blockchain and smart contracts. All access records are stored on the blockchain network. Decentralization of the access scontrol system is achieved using blockchain technology without the requirement for a central authority to be trusted.

A literature survey in section II and a proposed model in section III are also included in this work. The proposed model section describes the methodologies and as well as the system architecture that our suggested system implemented in order to create a blockchain application. We've come to an end with our paper in section IV and references.

2. Literature Survey

Patients should have easy access to complete and accurate medical records. As a healthcare provider, it is critical to ensure that patient's privacy is protected and medical records are stored securely. Personal medical records have long been a source of worry for the general population. With advent of blockchain technology, this issue can now be resolved. Personal medical records can be stored securely using blockchain technology, which is decentralised and verified. A blockchain-based cloud storage solution for personal medical data management is proposed in this study. Medical records sharing services are also discussed in this article**.** In addition, the differences between the medical blockchain and more traditional solutions are demonstrated and appraised. The suggested preserving andsharing system does not rely on any third parties, and no singleentity has complete control over processing.[1]

A plethora of knowledge about the healthcare industry can only be gained by having easy access to healthcare data. As a result, medical databases will grow in size, complexity, heterogeneity, and speed. Data storage and processing must be done in a way that will benefit humanity, and this is the most critical issue right now. Health care data is a huge concern for academics since it is so diverse. For this type of data, "big data" is a term that is sometimes employed. On their own, the Blockchain and the Cloud have shown their value. However, merging these two technologies opens up new and exciting possibilities in the healthcare industry. Networks of computers known as "nodes" are the basis of Blockchain's decentralisation and security. As a result, it's altering the way medical records are stored and shared. Data security and correctness can be monitored and maintenance expenses can be reduced by using it. A Blockchain-based technology has been proposed to preserve and retrieveelectronic medical records in the cloud. [2]

Security, massive traffic, high availability, and high dependability are just some of the challenges that must be overcome while creating Internet of Things (IoT) applications. Distributed computing concepts like software-defined networking (SDN), network virtualization, and blockchain can beused in conjunction or individually to address the aforementioned difficulties in IoT networks to some extent. For latency sensitive IoT applications, fog nodes are utilised in an SDN network-controlled edge computing layer to assure high reliability and availability In the SDN network, controllers and OpenFlow switches are dispersed. Blockchain technology can be used to establish reliable decentralisation. Not only that, but An all-network traffic model has been put out. The novel approach is tested in detail using simulations and a real-world testbed. The proposed framework, according to the findings of the experiments, improves latency and resource consumption efficiency. [3]

A decade ago, people began to hope that the Intelligent Transportation System(ITS)would be a reality as current vehicle and communication technologies evolved rapidly. The goal of ITS is to make transportation systems safer and more efficient by integrating information technology into them. However, security is still a key worry when it comes to vehicle communication systems (VCSs). Use a secure broadcast to communicate with your colleagues. As a result, key management techniques are regarded as critical to network security. This paper proposes a secure key management system for heterogeneous networks. Vehicle departure information, package block-to-transport keys, and subsequent rekeying on vehicles within the same security domain are all collected by the framework's security managers (SMs). This system's first component is a new network topology based on a decentralised blockchain structure. The blockchain approach simplifies distributed key management across disparate VCS domains. Using a dynamic transaction collection period, a second aspect of the framework speeds up the transfer of the vehicle's keys. According to a wide range of research, the framework under consideration is both effective and efficient, with a dynamic scheme allowing SMs to adapt to shifting traffic levels and a blockchain-based system surpassing the central manager-based system. [4]

The work of Young Gangan, Z et alconsidered blockchain to be a verifiable, accountable and eternal storage supply chain. These unique characteristics can be a feasible choice for healthcare facts networks which might be worried with each affected person protection and facts sharing. Thus, this study proposes an information base plan and software machine constructed at the block chain for saving, trading, and the usage of clinical facts.[5]

A study by Nisarga, B.L et al have proposed a high level half breed danger avoidance structure with a surveillance system that uses IoT technology to reduce most of human communication. This is a low-cost option due to the use of microcontrollers and cheap sensors. Future work will be joined with an insightful framework that that couldexpect danger in advance. [6]

A extensivequantity of study through Murugan et al have presented a blockchain-empowered framework for medical data sharing that addresses issues like records precision and coordination. Integrating the blockchain with HIE will give you access to accurate health data from the past. [7]

Anoopetal. in the case of the proposed method is a library book recommender framework that works with the effective completion of library day to day operations. This site makes a mechanism for administrators to store and retrieve books from the database. In this cloud-based library suggestion framework that utilizations appropriated separating algorithms, administrators add books based on category and suggest top-class books as well. [8]

King, H. Their work encourages to integrate IoT, blockchain and cloud technologies into your healthcare framework to give medical care and telemedicine. Enables secure following of patient crucial signs in smart hospitals or explicit areas. [9]

3. Proposed Model

It has shown that most of the effort has been kept to protecting and increasing encryption of heterogeneous and huge data. Despite this, servers are notoriously unstable, and valid privacy concerns arise as a result. We've used Blockchain technology to encrypt IoT data using an updated Hashing algorithm since SHA-512 is more durable and trustworthy as far as the time it takes to figure a solitary hash compared to all previous hash capacities.

A blockchain network is first created by the user or administrator, and then data from an IoT device is submitted using the SHA-512 hashing technique. Afterwards, different index values are applied to the same block of data in order to increase its value. The user's name and the date and time of the historical data post have been displayed using Resync. Our solution depends on blockchain technology to protect cloud-based heterogeneous and massive data. All data should be stored on a blockchain, which is more secure than a single database. Efforts to prevent database attacks from causing harm are made. Thus, a front-end platform for the user interface was created.

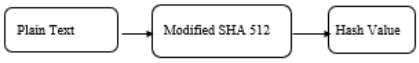

Fig 2: Structure of SHA512

Because of Hashing technique is more resilient and creates irregular strings to forestall data replication, a future aggressor would need additional opportunity to brute force a database hashed password. SHA512 is regarded more secure and stable than other hash techniques as it takes long time to generate a specific hash. SHA-512 is more secure than MD5 despite its slower speed for a multitude of reasons. Because of the 160-bit digest, bruteforce attacks are substantially more difficult. SHA-512 was chosen for implementation due to its high throughput of 512 bits.

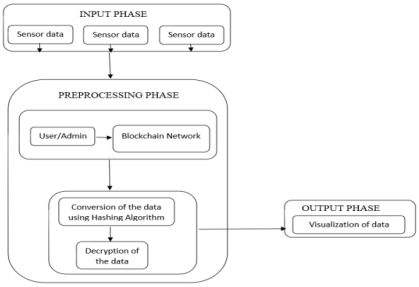

Fig 3: Block Diagram of the model

A hash function cannot distinguish two unique sets of inputs that produce the identical output in the absence of collisions (hash digest). We were able to enhance the visual appeal of our application's web pages. As soon as a POST request is sent to an unconfirmed node, our framework uses an HTML type to collect user information and attach it to the collection. Peer-to-peer transactions are made possible by the Blockchain protocol, which is a decentralised peer-to-peer network of devices that runs a copy of the Blockchain convention and maintains an similar duplicate of the exchange record. The blockchain uses SHA-512, a cryptographic hash function, to encrypt and connect the data that is constantly monitored. When it comes to cloud computing security, Blockchain is an excellent choice because it is both appropriate and robust. We do this in order to place some restrictions on the system. For the stack, we added a limit of two zeroes in our hash instead of taking any. When a block's content is altered, its hash will likewise be altered.

We don't have any IOT devices to sense data so we are generating random values as simulation to be consider as data and this data will be stored at Blockchain server and to access this data users has to register and then login and then only can access data. We have used Ethereum Blockchain server to store this data and to do so we need to develop and deploy solidity contract on Ethereum and this solidity will contains functions to store and access IoT data.

4. Result

For our blockchain decentralised application, we are improving its security and efficiency by altering its cryptographic hashing algorithm. When it comes to security, it would take longer for a future attacker to build all of the SHA512 hashes available to savage power a database secret phrase. When it comes to computation time for only one hash, SHA512 is better to all other algorithms.Inorder to improve the security we are encrypting the hash code by using the AES encryption algorithm.

Fig 5: Hashcode of SHA512

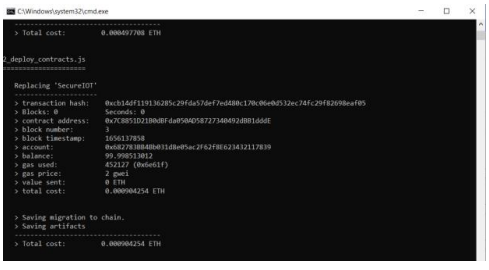

Fig 6: Deployment of Contract

In above screen we can see contract deployed and we got contract address and this address we will specify in python code to access that contract to store data.

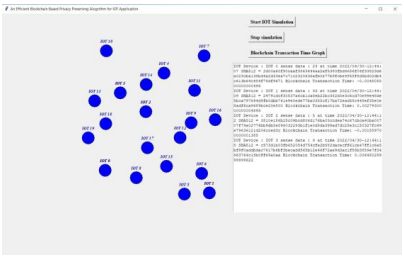

Fig 7: Hashcode and encryption

In above screen each circle we are considering as an device and whenever any data is generated andsend data to Blockchain then its colour will change to red and in text area we can see generated data and SHA512 hash code and the encrypted data of the hashcode.

5. Conclusion

In this project, a blockchain network was built and IoT data was safeguarded using Blockchain technology. We've created a decentralised blockchain software to store and protect the data which is randomly generated. Recently, a slew of more trustworthy hashing algorithms have been accessible. SHA-256, SHA-384, and MD5 are among them. When it comes to security, it would take longer for a future attacker to build all of the SHA512 hashes available to brute force a database password. When it comes to computation time for only one hash, SHA512 is better to all other algorithms.Once the hashcode is generated,inorder to provide the security to the data we are using encryption algorithm to encrypt the hashcode of the data.For our blockchain decentralised application, we are trying to improve its security and efficiency by altering its cryptographic hashing algorithm.

6. References

[1] Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2019). Blockchain-based medical records secure storage and medical service framework. Journal of medical systems, 43(1), 1-9.

[2] Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K., & Chang, V. (2018). A proposed solution and future direction for blockchain-based heterogeneous medicare data in the cloud environment. Journal of medical systems, 42(8), 1-11.

[3] Muthanna, A Ateya, A., Khakimov, Gudkova, Abuarqoub, A., Samouylov, K., & Koucheryavy, A. (2019). Secure and reliable IoT networks using fog computing with software-defined networking and blockchain. Journal of Sensor and Actuator Networks, 8(1), 15.

[4] Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., & Sun, Z. (2017). Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal, 4(6), 1832-1843.

[5] Yangang, Z., & Zhiyi, D. (2020). Research on the Application of Smart Rural Governance Platform Based on Blockchain Technology in Rural Sustainable Development. Revista Argentina de Clínica Psicológica, 29(5), 1339-1349.

[6] Nisarga, B. L., Manishankar, S., Sinha, S., & Shekar, S. (2020). Hybrid IoT-based Hazard Detection System for Buildings. In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 889-895). IEEE

[7] Murugan, A., Chechare, T., Muruganantham, B., & Kumar, S. G. (2020).Healthcare information exchange using blockchain technology. International Journal of Electrical and Computer Engineering, 10(1), 421.

[8] A. Anoop and N. A. Ubale, "Cloud-Based Collaborative Filtering Algorithm for Library Book Recommendation System," 2020 Third InternationalConference on Smart Systems and Inventive Technology (ICSSIT), 2020, pp. 695703, DOI:10.1109/ICSSIT48917.2020.9214243

[9] Wang, H. (2020). IoT-based Clinical Sensor Data Management and Transfer using Blockchain Technology. Journal of ISMAC, 2(03), 154-159.

[10] Hui Lia, Tao Jing, A Ciphertext-Policy Attribute-based Encryption Scheme with Public Verification in 2019 international Conference on Identification, Information and Knowledge in the Internet of Things. 10.1016/j.procs.2020.06.080.

[11] Norisvaldo Ferraz Junior Anderson, A.A. SilvaAdilso, Privacy-preserving cloud-connected IoT data using context-aware and end to-end secure messages in 18th International Conference on Mobile Systems and Pervasive Computing, Volumuyjjhyhe 191 10.1016/j.procs.2021.