ABSTRACT

Over the past few years, the Internet of Things (IoT) has gained immense importance in our lives, being extensively utilized in various domains to simplify business operations and day-to-day activities. However, apprehensions regarding security and safety have surfaced, leading researchers to focus on finding optimal remedies to heighten security and privacy. One such solution is the integration of blockchain technology with the IoT. Nowadays, blockchain-based Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has been proposed to achieve secure IoT data sharing. The devices of the IoT are expected to gather vast amounts of data to support various applications such as health monitoring, smart homes, and traffic management.

When sharing data through blockchain-based CP-ABE, the information undergoes encryption and is kept in the cloud. Users must download and decrypt the ciphertext on the client end before handling the data. Following processing, the users upload the ciphertext back to the cloud and encrypt it. Unfortunately, there are no advantages to employing cloud computing resources with this strategy. This problem can be handled by calculating the ciphertext and using Fully Homomorphic Encryption (FHE) and homomorphic signature techniques to confirm the accuracy of the numerical results. A secure and efficient IoT data exchange system is presented, allowing users to take advantage of the simplicity of cloud-end computation. The proposed system integrates FHE and CP-ABE to enable secure IoT data sharing and ciphertext calculation. Moreover, users can verify the accuracy of the computation results by producing homomorphic signatures for the ciphertexts. In order to monitor cloud storage and offer consumer-trusted IoT data access control, the data access policy, hash, ciphertext signature, and homomorphic signature on the blockchain should be authorized.

In contemporary times, it is imperative to collect information with restricted energy usage and robust security measures in place. The network's energy output is restricted due to the use of battery-powered sensor nodes. The nodes within the network are susceptible to various forms of attack, and therefore, the suggested method of data transmission must guarantee network protection.

The first method presents a secure method for aggregating data that incorporates compression techniques and encryption using blockchain-based routing. A hash key produced with the help of a Spider Web-based Dynamic Key generation mechanism (SWDK) is merged with the receiver of the device to assure security. The compressed data with SWDK is then transferred through the blockchain encryption routing process. Data aggregation using compression is then used to reduce the data transmission costs and their sizes. The network devices send data to the server or Base Station (BS) through gateways. Simulating results demonstrate that this proposed method reduces transmission costs and energy consumption compared to existing methods. Additionally, network throughput is improved through the sharing of security keys.

The second method proposes a blockchain-dependent data transfer scheme. It employs homomorphic encryption, ensuring the security of data collection and transfer when monitoring network systems. Homomorphic encryption is utilized to encrypt and ensure that the original data that has been decrypted is the same as the original data. An IoT device gathers the encrypted asymmetric public key for executing the blockchain-based data secure assignment design. The blockchain-based enhanced encryption allows for decentralization, which solves the trust issue. This makes IoT data aggregation on the blockchain a sensible option for creating a system that protects user privacy.

A compression-based IoT data aggregation strategy can help achieve this goal, and blockchain-based encryptions along with routing skills are intended. The Prey localized Spider Orb Web-Dependent Dynamic Key (PSWDK) generation process is used to create a hash key, and the compressed data is exchanged during the blockchain encrypted routing procedure. A new technique is proposed for the detection procedure using the spider's legs as different sensors at the distribution point. Because of its excellent transmission accuracy and short transmission duration, this technique effectively eliminates data manipulation due to prolonged transmission time. Every data user has the ability to draft a smart contract and expose more than just the terms of service but also the desired data in IoT in the suggested system. The transfer scheme employed in the approach is more consistent than the previous transfer technique. Further, it does not frequently undergo data distortion, in contrast to the management method utilized in this module.

In the final part of the thesis, an innovative strategy is suggested to preserve the privacy of IoT devices. It utilizes the Privacy Set Intersection (PSI) and blockchain technology to safeguard data privacy. Initially, a PSI practice is proposed based on homomorphic encryption and 0-1 encoding, which effectively conceals the set base and ensures data privacy. Next, by integrating smart contract and blockchain structures, the proposed scheme enhances data sharing efficiency by keeping shared data on the blockchain. Our secured investigation shows that our pattern provides exceptional control over individual data, ensuring data security and privacy.

Our results show that the suggested solution performs significantly better than these other approaches with regard to encryption, key generation, and decryption times in multi-source data processing. This makes it a promising solution for an extensive range of applications. At the end, functionalities with other relevant systems are compared. The portions that came before it shows how good our system is at demanding little in the way of computation or transmission expenditures.