



SECURING IOT DATASET USING BLOCKCHAIN TECHNIQUE

¹Bhumika M G, ²Dr.Veena M N

¹PG Student, ²Professor

¹Department of MCA,

¹PES College of Engineering, Mandya, Karnataka, India

Abstract : IoT is still a relatively new concept, but it has a lot of potential in its early stages, it will soon have a significant impact on almost everything we use on a daily basis. The more it is associated with our way of life, the greater the likelihood that it will be mistreated. It is vital to protect IoT devices from breaking. Very soon, IoT will expand the territory for digital assaults on homes and businesses by integrating previously disconnected items into on-line frameworks. Existing security advancements are insufficient to address this issue. As a possible solution for future IoT frames, the Square Chain has emerged that are more secure. This article will primarily provide blockchain technology overview and implementation, then discuss IoT foundations based on blockchain organization, and finally discuss a blockchain-based model for IoT security.

IndexTerms - Internet of things, Blockchain, Security, Devices, Network.

I. INTRODUCTION

Today's scenario maintenance and using internet of things(IoT) data is increasing across all the domain. The data from different domain is freely available for different applications, securing this data is challenging. The solution for this is blockchain technique. By using this technique we can store a IoT data in a system that is impossible to change or hack the system.

The blockchain network's fundamental functions include peer-to-peer messaging, distributed data sharing, and consensus - which provides proof of work. Shared ledger - When a transaction occurs, the ledger is updated. It is publicly available and is incorruptible which introduces transparency to the system. Cryptography - it ensures that all information in record and organizations gets encoded and just approved client can unscramble the data and keen agreement - it is utilized to confirm and approve the members of the organization.

II. LITERATURE SURVEY

IoT is developing extremely quick and making its essence felt in pretty much every field of innovation. Nonetheless, with its quick development, it has made itself more inclined to digital assaults. Presently there is an earnestness to make IoT safer [1]. Web Of-Things (IoT) alludes to an inexactly coupled, arrangement of different heterogeneous what's more, homogeneous gadgets having the force of detecting, preparing, and network abilities [2]. Webs of Things have been talked about suitably with semantic touch in the IoT vision [3]. The development of the IoT makes a large number of devices, such as sensors, interconnection, and interoperability for data collection and exchange. By utilizing data from the Internet of Things, we can gain a better understanding of our environment [4]. On the other hand, the IoT is made up of devices that generate, procedure, and Exchange massive amounts of critical security and security information and personal information, making them attractive targets for cyber attacks [5]. Supporting security and privacy on a budget is a significant challenge, as many new networked devices that comprise the Internet of Things consume fewer energy, are lighter and memory is lower [6]. These devices must be dedicated performing critical application functions with the majority of their energy and computation resources [7]. Numerous researchers have contributed to their development. The transmission field is included in the security research [8, 9], field of cloud storage [10, 11], field of digital signatures [12, 13], and field of permission identification [14, 15].

III. PROPOSED METHODOLOGY

In the proposed work we have developed a system to secure IoT data. In the proposed model IoT data set has been uploaded through network nodes. The data in the one node copied to every other nodes within the network. It eliminates the central authority. The data is transparable to all the clients. Each node is made with a special functionalities like smart contract, consensus, shared ledger and cryptography. The trustworthy blockchain is designed with SHA 256 Algorithm so no one can edit the data and it is highly difficult or impossible to change the data within the network.

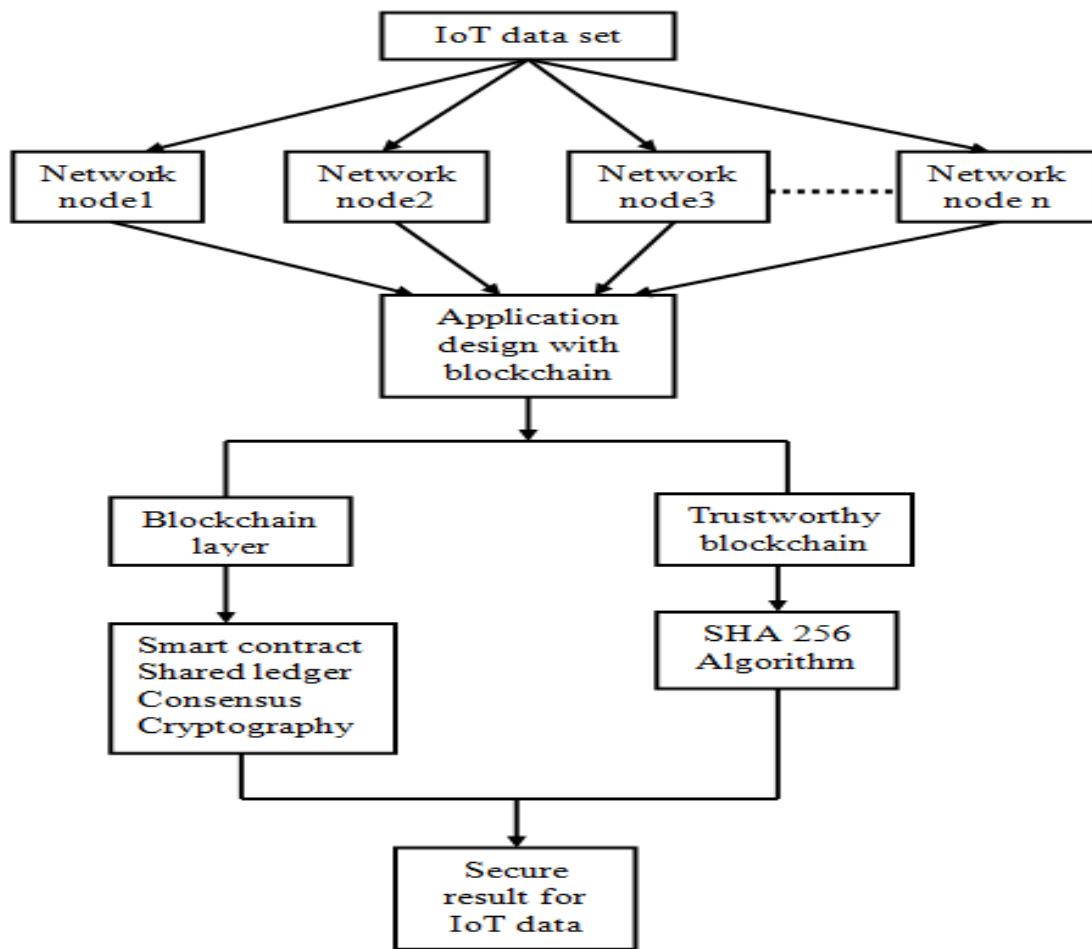


Figure 3.1: Proposed Model

IV. ALGORITHM

3.1 SHA 256

The secure hash algorithm is a subset of the cryptographic hash function family. A hash is a type of 'signature' for a text or data piece. SHA-256 generate an almost sole 256-bit signature (32-byte). A hash in the conventional sense is not "encryption;" The original text cannot be decrypted back.

Steps:

1. Pre-Processing: Convert text to binary. Add 0's to a single 1 Pad up to 512, but less than 64 bits for the data. Add 64 bit to the end, where the 64 bits represent the binary length of the original input in big-endian format.
2. Initialize Hash Values (h): Now we're going to generate eight Values of hash. These are constants called as hard-coded constants representing the first 32 bits of the first 8 square roots of the fractions: 2, 3, 5, 7, 11, 13, 17, 19
3. Start Round Constants (k): In the same way as step 2, we are going to initialize some constants. This time there are 64 of them. The first 32 bits of fractional portions of the first 64 cube roots(2-311) are represented by each value (0-63).
4. Chunk Loop: Divide the padded binary into 512bit chunks. Divide each chunks into 32bit word per chunk
5. Create a Schedule for Messages (w): Copy the data to a new array from step 1 with 32-bit entries. Add 48 additional words that are initialized to zero, creating an array $w[0..63]$.
6. Compression: Then initialize each variable (a, b, ..., h) to its hash value. $h_0, h_1, h_2, \dots, h_7$. Run the compression loop.
7. Change Final Values: Following the compression loop but within the chunk loop, By adding the required variables (a-h) we update the Hash values. the entire add-ons are modulo 2^{32} as usual.
8. Summon the Hash Final: At the end, hit them all together with a simple concatenation string.

3.2 Support Vector Machine Algorithm

The Support Vector Machine, also called SVM, is a supervised algorithm for learning commonly using in categorization, regression issues and it is primarily used in Machine Learning for Classification problems.

Text categorization:

SVM used in training models that are used to classify the IoT documents into different categories based on location.

Steps:

1. Import the IoT dataset
2. Explore the IoT data to find out how they look like
3. Pre-process the data
4. Split the IoT data into attributes and Location as labels
5. Divide the IoT data into training and testing sets

6. Train the SVM algorithm
7. Classify the IoT data based on location
8. Evaluate the results of the algorithm using bar chart.

V. EXPERIMENTAL RESULTS

The implementation of the project is to teach management the right way to receive accurate information from the computerized system, as well as to make data entry easier and error-free. It contributes to a more secure and reliable Internet of Things model. It lowers the cost of building massive internet infrastructure.

1. Datasets

Here we can see the IoT data files uploaded in the network. We can download the data whichever we want by using hash code.

File Name	Description	Upload File	Location	Hashcode Request	Download Page
report	seminar report	Final_Report.docx	chennai	send	send
agriculture	agriculture data	API_1_DS2_en_csv_v2.csv	mandya	send	send
agriculture	survey	API_1_DS2_en_csv_v2_ZotcL9M.csv	bengaluru	send	send
mandya	traffic details	Metadata_Country_API_1_DS2_en_csv_v2.csv	mandya	send	send
agricluture	agriculture data	Metadata_Indicator_API_1_DS2_en_csv_v2.csv	mandya	send	send
traffic	mandya city	API_1_DS2_en_csv_v2.csv	mandya	send	send
agriculture2	mysore data	API_1_DS2_en_csv_v2_GImvDWa.csv	chennai	send	send

Figure 5.1 : IoT Dataset Page

2. Hash code validation

In the datasets page clients request the system to download the files. The system will sent the 256 bit length hash code to clients Email that will be validated here.

please enter hash code value

submit

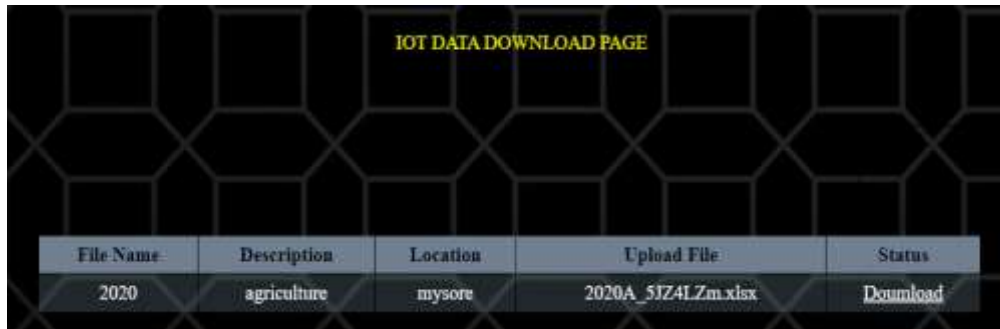
V1P7X6C5DP8SIOHSC9MP8WQPLK1B62GDFRJS1MUX8NTL7TW29PWW4V

V2OUKWAKQ6TU8QZ40E66WD66UIU41PN8L4ZZPMMMAOSORNIB5U2260E

Figure 5.2 : Hash Code Validation Page

3. IoT data download

Here system gives permission to download the IoT data after all the credentials validated.



File Name	Description	Location	Upload File	Status
2020	agriculture	mysore	2020A_5JZ4LZm.xlsx	Download

Figure 5.3 : IoT Data Download Page

4. Bar chart

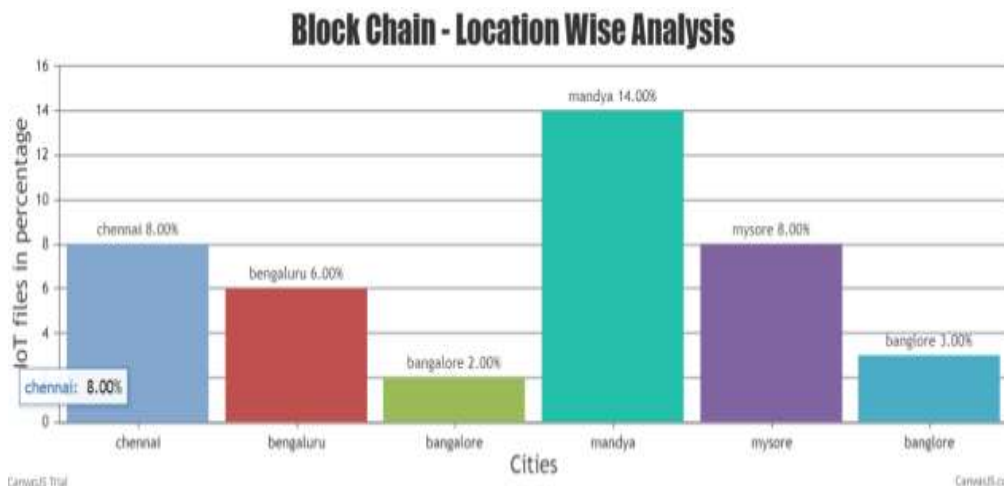


Figure 5.4 : Analysis of IoT Data Based on Location

VI. CONCLUSION

This proposed work provides use of blockchain technology guidance by way of case studies in order to create a most protected and trustworthy model for IoT. Because of the high-end hardware needs, we concluded that IoT will not be complete blockchain network member.

The proposed model provides an overview of blockchain technology, discusses security concerns in the IoT environment, and also proposes an IoT security solution.

REFERENCES

- [1]. Singh, Dhananjay, Gaurav Tripathi, and Antonio J. Jara. "A survey of Internet-of-Things: Future vision, architecture, challenges and services." Internet of Things (WF-IoT), 2014 IEEE World Forum.
- [2]. Atzori, and Morabito, —The internet of things: A survey, Computer Networks, 54(15), 2787– 2805, 2010.
- [3]. Humayed, Abdulmalik, "Cyber-Physical Systems Security—A Survey." arXiv preprint arXiv:1701.04525 (2017).
- [4]. Y. Zhang and J. Wen, "Te IoT electric business model: Using blockchain technology for the internet of things," Peer-to-Peer Networking and Applications, vol. 10, no. 4, pp. 983–994, 2017.
- [5]. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Tings: the road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.
- [6]. R. Xie, C. He, D. Xie, C. Gao, and X. Zhang, "A Secure Ciphertext Retrieval Scheme against Insider KGAs for Mobile Devices in Cloud Storage," Security and Communication Networks, vol. 2018, pp. 1–7, 2018.
- [7]. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: Te case study of a smart home," in Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017, pp. 618–623, IEEE, Kona, HI, USA, March 2017.
- [8]. L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure Multiple Amplify-and-Forward Relaying with Cochannel Interference," IEEE Journal of Selected Topics in Signal Processing, vol. 10, no. 8, pp. 1494–1505, 2016.
- [9]. L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secrecy Cooperative Networks with Outdated Relay Selection over Correlated Fading Channels," IEEE Transactions on Vehicular Technology, vol. 66, no. 8, pp. 7599–7603, 2017.
- [10]. J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloudaided lightweight certificateless authentication protocol with anonymity for wireless body area networks," Journal of Network and Computer Applications, vol. 106, pp. 117–123, 2018.
- [11]. Z. Wu, L. Tian, P. Li, T. Wu, M. Jiang, and C. Wu, "Generating stable biometric keys for flexible cloud computing authentication using finger vein," Information Sciences, vol. 433–434, pp. 431–447, 2018.

- [12]. Q. Lin, J. Li, Z. Huang, W. Chen, and J. Shen, "A short linearly homomorphism proxy signature scheme," *IEEE Access*, vol. 6, pp. 12966–12972, 2018.
- [13]. M. Tao, K. Ota, M. Dong, and Z. Qian, "AccessAuth: Capacityaware security access authentication in federated-IoT-enabled V2G networks," *Journal of Parallel and Distributed Computing*, 2017.
- [14]. J. Li, L. Sun, Q. Yan, Z. Li, W. Srisa-an, and H. Ye, "Significant Permission Identification for Machine Learning Based Android Malware Detection," *IEEE Transactions on Industrial Informatics*, vol. PP, no. 99, pp. 1-1, 2018.
- [15]. J. Chen, K. He, Q. Yuan, G. Xue, R. Du, and L. Wang, "Batch Identification Game Model for Invalid Signatures in Wireless Mobile Networks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 6, pp. 1530–1543, 2017.

