IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⵘ Impact Factor 7.047 ⵘ Vol. 10, Issue 9, September 2022

DOI: 10.17148/IJIREEICE.2022.10913

A Secure Block chain-Based Scheme for IOT Data Credibility in Fog Environment

Anusha K[1], Thouseef Ullah Khan[2]

PG Scholar (MCA), Dept. of MCA, Vidya Vikas Institute of Engineering and Technology, Mysore, Karnataka, India[1].

Assistant Professor, Dept. of MCA, Vidya Vikas Institute of Engineering and Technology, Mysore, Karnataka, India[2].

Abstract: Data sincerity plays a vital role in easing evidence-based decision making in organizations and governments (e.g., policy making) within a fog environment. One of the main data sources is the Internet of Things (IoT) devices and systems. The ecosystem of the manufacturing industry is expected to be activated through autonomous and intelligent systems such as self-organization, self-monitoring and self-healing. The Fourth Industrial Revolution is beginning with an attempt to combine the myriad elements of the industrial system with Internet communication technology to form a future smart factory. The related technologies derived from these attempts are creating new value. However, the existing Internet has no effective way to solve the problem of cyber security and data information protection against new technology of future industry. In a future industrial environment where a large number of IoT devices will be supplied and used, if the security problem is not resolved, it is hard to come to a true industrial revolution.

Keywords: Block Chai , IOT Data Credibility, Fog Environment, Block Chain for IOT, Secure Block Chain

I. INTRODUCTION

The mist climate can be considered as a momentary engineering between the discernment layer endpoints and the client's gadgets in the Internet of Things instance. Edge figuring is frequently confused for haze processing. But even so, there are some gentle contrasts between the two. The first, in particular haze registering, is considered as an exceedingly virtualized stage that interfaces cloud server farms and terminal designs, empowering them to process, stock and offer web-based types of assistance. A mist climate, as a general rule, comprises of key haze hubs that are associated with an assortment of (possibly unique) IOT gadgets inside various districts/confined regions, and these hubs are liable for briefly putting away the information gathered on the associated IOT gadgets (for example sensors). By large, the last option will identify, gather and send the information to the haze hubs for pre-handling, primer investigation and / or sending to the cloud server for additional information examination. Subsequently, it empowers more imaginative and complex huge information examination (e.g., information gathered from various haze conditions). Furthermore, hazy conditions further develop correspondence proficiency and offer better help for ongoing applications. (for example in the vehicle's web settings and wellbeing/care settings, ongoing information sharing and direction is conceivable).

II. EXISTING SYSTEM

Law et al. proposed a key management phase (WAMS) to accomplish the invulnerable objectives for the information transformations. To carry out validation in specially designated nearby remote organizations, Balfanz et al. proposed an appropriately evaluated, easily understood and protected provision in which pre-validation is achieved through actual contact in a somewhat restricted channel. Han et al. devised a plan to patrol the rebel passages in foggy conditions. Specifically, the full circle time in the middle of DNS servers and end clients will help to identify unauthorized gateways.
Title: Able key administration plot for multicast bunches utilizing bunch key understanding and broadcast encryption

Authors: E. Abirami; T. Padmavathy

This task proposes another key administration worldview, which consolidates conventional transmission encryption and gathering key arrangement, which never uncovers dynamic gathering data to pariahs and accomplishes both direct mystery and in reverse mystery. It furnishes a solid key administration model with the general population and confidential key, yet in addition two other keys called bunch key and meeting key. Nonetheless, existing arrangements might be incapable against new or arising security assaults in cloud conditions, especially as how much information to be filtered increments.

Title: HIDRA: A blockchain-based distributed architecture for Fog / Edge Computing environments

Authors: Carlos Núñez-Gómez; Blanca Caminero; Carmen Carrión

The widespread idea of haze calculation makes resource coordination a test. In general, the mixed agreements involved are of limited use in this specific situation. Additionally, cloud centers are often tied to resources, so running management modules must be carefully planned together so they don't cause unnecessary overhead. On the other hand, block chain has proven its usefulness beyond digital currencies, to help store solid and widespread data. When combined with smart agreements, it can lead to a PC in circulation where all centers add freely and in a similar fashion to a standard global framework state, which must be mutually agreed upon. This also provides inherently beneficial highlights such as immutable nature and simplicity.

Title: Fog based document sharing for secure and proficient record the executives in an individual organization with heterogeneous cell phones.

Authors : Jung-Eun Park; Young-Hoon Park

This document sharing was planned disregarding a heterogeneous wearable gadget. To beat the above issues, we initially propose another fog network model that designates the calculation for planning record capacity and recovery to a fog hub, for example, a cell phone or tablet. A haze hub has a relatively quicker functional limit and more noteworthy battery limit, and consequently the assets of the gadgets in the PAN can be overseen proficiently. The proposed arrangement won't give effective, secretive and versatile access control to work with information partaking in haze and cloud conditions.

Drawbacks of existing system:

1. In the existing work, the system does not provide secure Techniques based on block chains.
2. In the existing work, the system does not provide secure Techniques based on block chains.

III. PROPOSED SYSTEM

Information Aggregation: regulate the Block chain attributes where the gadget is in. In the event that it is on the confidential chain, no one but hubs can get to and control the information. Assuming that it is on the public chain, the information of this hub should be distributed on the public Block chain. The adding information capability is called in light of the worth and the Devfp address, & to produce a block, the recently added information should be stocked.

Question on information: The enquiry capability here just alludes to the information in the confidential chain. The items in the relating question will be returned in view of different block IDs.

Altering Data: This technique is like adding information; The block stores the changed information or an invalid value. In the event that there are no special cases in the past execution process, like lacking memory or break, then the execution was effective.

Advantages of Proposed System:

1. The proposed system enhances the evaluating and handling potentiality of edge networks.
2. The system has become more secure since the attribute-based signature algorithm was implemented.

DOI: 10.17148/IJIREEICE.2022.10913

IV. SYSTEM ARCHITECTURE

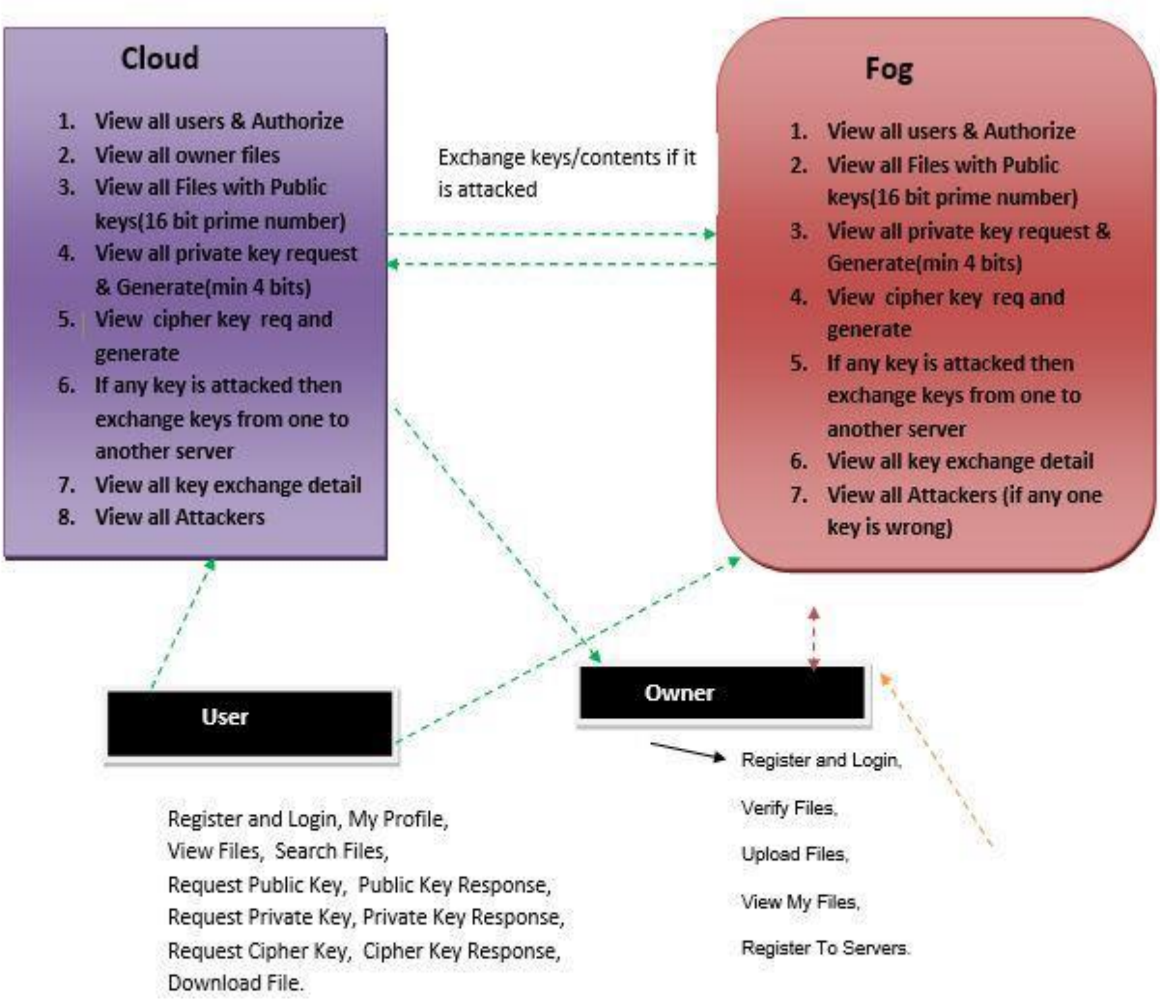
Cloud
1. View all users & Authorize
2. View all owner files
3. View all Files with Public keys(16 bit prime number)
4. View all private key request & Generate(min 4 bits)
5. View cipher key req and generate
6. If any key is attacked then exchange keys from one to another server
7. View all key exchange detail
8. View all Attackers
Exchange keys/contents if it is attacked
Fog
1. View all users & Authorize
2. View all Files with Public keys(16 bit prime number)
3. View all private key request & Generate(min 4 bits)
4. View cipher key req and generate
5. If any key is attacked then exchange keys from one to another server
6. View all key exchange detail
7. View all Attackers (if any one key is wrong)
User
Owner
Register and Login,
Verify Files,
Upload Files,
View My Files,
Register To Servers.
Register and Login, My Profile,
View Files, Search Files,
Request Public Key, Public Key Response,
Request Private Key, Private Key Response,
Request Cipher Key, Cipher Key Response,
Download File.

Fig. 1 System Architecture

V. MODULES

A. DATA OWNER :

1. Registration
2. Login
3. Upload File
4. View Uploaded File Details
5. Download
6. Logout

B. CLOUD SERVER :

1. Login
2. View User Details
3. View Attackers
4. View Files with public key
5. View Key Exchange Details
6. Logout
7. Logout

DOI: 10.17148/IJIREEICE.2022.10913

C. FOG SERVER :

1. Login
2. View User Details
3. View Attackers View Files with public key
4. Generate Private key and Cipher Key for the Files
5. View Key Exchange Details

D. END USER:

.

1. Registration
2. Login
3. View Cloud Files
4. Search Files
5. Request public key and view response
6. Request private key and view response
7. Request cipher key and view response
8. Download File
9. Logout

VI. CONCLUSION

The subject related to the security and protection of the IOT framework is many and need to be analyzed carefully. Both unified and decentralized agreements enjoy advantages and pitfalls. Adaptability limits embedded arrays, while delays, computational overhead, and power requirements limit decentralized approaches. To provide security components for decentralized and lightweight IOT access control, we proposed a multi-vendor framework. Block chain is responsible for providing the essential security to be in control, as well as matching neighboring IOT devices, fog centers, central fog centers, and distributed computing. We present our SBBS proposal to ensure the validity of information in foggy conditions. As described in this report, ABS allows for confirmation and Block Bind allows us to establish a strong matching climate to reduce the threats of information tampering and attain continuous synchronization. We also evaluate the safety and execution of the proposed plan to demonstrate its usefulness. Additional exploration will incorporate the proposed storyline simplification for further diverse conditions, as in a poorly organized environment (e.g., frontline IOT or military environments).

VII. FUTUTRE ENHANCEMENT

The proposed project will be implemented in a real-time environment in the future to evaluate the achievement of key security objectives, such as integrity via digital signature, authentication via shared secret keys, and authorization via MAC policy and confidentiality via key encryption. We will investigate various solutions to the problem of the large size of the block chain header. One possible solution is to separate the header block access control policy from the block structure in the block chain and store it in a separate block chain or cipher text file.

REFERENCES

[1] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog computing: A taxonomy, survey and future directions," in Internet of Everything. Singapore: Springer, 2018, pp. 103–130. [4] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.

[2] Z. Hao, E. Novak, S. Yi, and Q. Li, "Challenges and software architecture for fog computing," IEEE Internet Comput., vol. 21, no. 2, pp. 44–53, Mar./Apr. 2017.

[3] A.V. Dastjerdi et al., "Fog computing: Principles, architectures, and applications," in Internet of Things. Cambridge, MA, USA: Morgan Kaufmann, 2016, pp. 61–75.

[4] S. Sarkar, S. Chatterjee, and S. Misra, "Assessment of the suitability of fog computing in the context of Internet of Things," IEEE Trans. Cloud Comput., vol. 6, no. 1, pp. 46–59, Jan.–Mar. 2018.