WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Survey on A User Authentication Scheme Using Block Chain-Enabled Fog Nodes

[1]Sumit Dange, [2]Prajwal Mundre, [3]Prof. Prerna Jaipurkar

[1]Information Technology Department, SMT. RadhikataiPandav College of Engineering, Nagpur, India
[2]Information Technology Department, SMT. RadhikataiPandav College of Engineering Nagpur, India
[3]Information Technology Department, SMT. RadhikataiPandav College of Engineering Nagpur, India
DOI: https://doi.org/10.55248/gengpi.234.4.38223

ABSTRACT —

The main objective of this project is securely store and maintain the data using block chain.The blockchain technology is used to protect the healthcare data hosted within the cloud. The block that contain the data and the time stamp.It allows healthcare provider to access the IOT data more securely from anywhere. we propose a user authentication scheme using block chain-enabled fog nodes in which fog nodes interface to Ethereum smart contracts to authenticate users to access IoT devices. Block chain is fundamentally a decentralized, distributed, shared, and immutable database ledger that stores registry of assets and transactions across peer-to-peer (P2P) network It preserve data from attackers. The data is encrypted prior to outsourcing to the cloud. The healthcare provider have to decrypt the data prior to download.

Keywords — Key, Security, IoT, File storage, file management, Fogg computing.

I. Introduction

IoT devices are being deployed at a massive scale, with Cisco predicting 20 billion devices by the year 2020. As opposed to endpoint devices, IoT devices are resource constrained devices, and are incapable of securing and defending themselves, and can be easily hacked and compromised.Therefore, it is important to adopt proper schemes for authentication and control access to ensure the overall security for IoT devices, their communications, and their data Any proper user authentication scheme to IoT devices must consider the fact that IoT devices are resource-constrained devices and unable to carry out heavy processing and computation. Also the authentication scheme must be reliable, scalable, and secure against known attacks and threats. Furthermore, fog computing has emerged as a new computing paradigm that has the ability to perform localized processing, storage, and analytics for a group of IoT devices. Many IoT solutions have now been put forth by researchers in utilizing the fog nodes to relieve IoT devices from some of the heavy processing computational workload. Moreover, research communities as a distributive technology that is poised to play a major role in managing, controlling, and most importantly securing IoT devices. Blockchain can be a key enabling technology for providing viable security solutions to todays challenging IoT security problems. To date, most authentication techniques for IoT systems are centralized in design and deployment, and rely on a Trusted Third Party to authenticate the entities such as Open Authorization (OAuth) protocol. This approach has drawbacks such as high cost, being a single point of failure, hacking, and privacy evasion. To overcome the drawbacks of the centralized based authentication, a decentralized authentication scheme using fog nodes and blockchain technology is proposed in this paper. This scheme facilitates managing and accessing IoT devices while providing security without the need of a Trusted Third Party. Additionally, the proposed work involves the use of new architectures including edge computing and block chain, which facilitates performing authentication at scale, by taking advantage of fog node deployment. The primary goal of this paper is to propose and analyze the security of a blockchain-based authentication scheme at scale For IoT devices. Specifically, we present an architecture and design of a system involving end users, IoT devices, fog and cloud nodes, as well as Ethereum Blockchain smart contracts which govern the authentication rules and logic. The primary contributions of this paper can be summarized as follows: We propose a decentralized and scalable authentication mechanism that utilizes blockchain-enabled fog nodes with connectivity to Ethereum smart contracts for authenticating user access to IoT devices whereby access tokens are issued by the smart contracts with no intermediary or trusted third party.

II. Problem Statement

Large organizations and businesses generate a significant amount of data that needs to be stored, processed, and analyzed regularly. As the amount of data increases, traditional cloud computing solutions may not be able to handle the data processing and storage requirements. Additionally, data privacy and security concerns have made it difficult for organizations to trust third-party cloud providers to store and process sensitive data.

Furthermore, organizations need to manage and store data from multiple locations and devices, which can be a cumbersome task. Traditional file management systems may not be able to keep up with the pace of data generation and storage needs.

III. Objective

Fog computing is a distributed computing architecture that aims to provide computing resources closer to the end-users and data sources, improving data processing speed and reducing network congestion. The primary objectives of using fog computing are:

1. Reduced Latency: By deploying fog computing nodes closer to the data sources, the data processing and analysis can be performed more quickly, reducing the overall latency and improving the responsiveness of applications and services.
2. Improved Bandwidth Efficiency: With fog computing, the data can be processed and analyzed closer to the source, reducing the need for transferring large amounts of data to the cloud. This approach can significantly reduce network congestion and improve bandwidth utilization, leading to a more efficient use of network resources.
3. Increased Security: Fog computing can provide an additional layer of security to the data processing and analysis process. By distributing computing resources across multiple edge devices, data can be stored and processed locally, reducing the need to transfer sensitive data to the cloud. This approach can help organizations to better protect their data from unauthorized access and reduce the risk of data breaches.
4. Better Scalability: Fog computing can provide a highly scalable architecture that can handle large volumes of data generated by IoT devices and other data sources. The distributed nature of fog computing enables the addition of new nodes to the network, allowing for increased processing power and storage capacity as the data volume grows.
5. Lower Costs: By using fog computing, organizations can reduce their cloud computing costs by performing data processing and analysis locally, reducing the amount of data that needs to be transferred to the cloud. Additionally, the distributed nature of fog computing can reduce the need for expensive centralized data centers, leading to lower infrastructure costs.

IV. LITERATURE SURVEY

- Outsourced symmetric private information retrievalS. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, and M. Steiner

Outsourcing is the process of contracting an existing business process which an organization previously performed internally to an independent organization, where the process is purchased as a service. The data owner enables SSE Scheme and outsources a document or collection of files to a remote server in encrypted form. And also the data owner authorizes clients (third parties) to search the database to learn. The remote server still does not learn about the data or queried values as in the basic SSE setting. We extend the OXT protocol of Cash et al. to support arbitrary Boolean queries in all of the above models while withstanding adversarial non-colluding servers (Data owner and remote server) and arbitrarily malicious clients to preserve the remarkable performance of the protocol.

Advantages

- ✔ Implementing digital signatures.
- ✔ Cryptographic protocols with different security and privacy features.
- ✔ Supporting various signature schemes without adding additional hardware complexity compared to a hardware implementation of a conventional signature scheme.

Disadvantages

- ✔ Encryption keys aren't simple strings of text like passwords
- ✔ Damage is massive when you lost your symmetric key

- Dynamic search-able symmetric encryptionS. Kamara, C. Papamanthou, and T. Roeder

Searchable symmetric encryption (SSE) allows a client to encrypt data in such a way that it can later generate search tokens to send as queries to a storage serve. We propose the first SSE scheme to satisfy all the properties like sub-linear search time and so-on. Extends the inverted index approach in several non-trivial ways and introduces new techniques for the design of SSE. We implement our schemeand conduct a performance evaluation, showing that our approach ishighlyefficient and ready fordeployment.

Advantages

- ✔ Security against adaptive chosen-keyword attacks.
- ✔ Compact indexes.
- ✔ Ability to add and delete files efficiently.

Disadvantages

- ✔ Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only secure way of exchanging keys would be exchanging them personally.

- Highly-scalable searchable symmetric encryption with support for Boolean queries

  D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, andM. Steiner

The design, analysis and implementation of the first searchable symmetric encryption (SSE) protocol that supports conjunctive search and general Boolean queries on outsourced symmetrically-encrypted data and that scales to very large databases and arbitrarily-structured data including free text search. Our solution provides a realistic and practical trade-off between performance and privacy by efficiently supporting very large databases at the cost of moderate and well-defined leakage to the outsourced serve.

Advantages

- ✔ Providing performance results of a prototype applied to several large representative data sets, including encrypted search over the whole English Wikipedia.

- ✔ Load Balancing

Disadvantages

- ✔ Exact matching may retrieve too few or too many documents.

- Practical dynamicsearchable encryption with small leakageE. Stefanov, C. Papamanthou, and E. Shi

DynamicSearchableSymmetricEncryption(DSSE) enables a client to encrypt his document collectionin a way that it is still searchable and efficiently updatable. We propose the first DSSE scheme that achieves the best of both worlds,i.e., both small leakage and efficiency. Our scheme leakssignificantly lessinformation than any otherprevious DSSE construction and supports both updates andsearches in sub-linear timein the worst case, maintaining atthe same time a data structure of only linear size. We finallyprovide an implementation of our construction, showing itspractical efficiency

Advantages

- ✔ Complete expressiveness for any identifiable subset of collection.

- ✔ A symmetric cryptosystem uses password authentication to prove the receiver's identity

Disadvantages

- ✔ Cannot provide digital signatures that cannot be repudiated

V. DFD

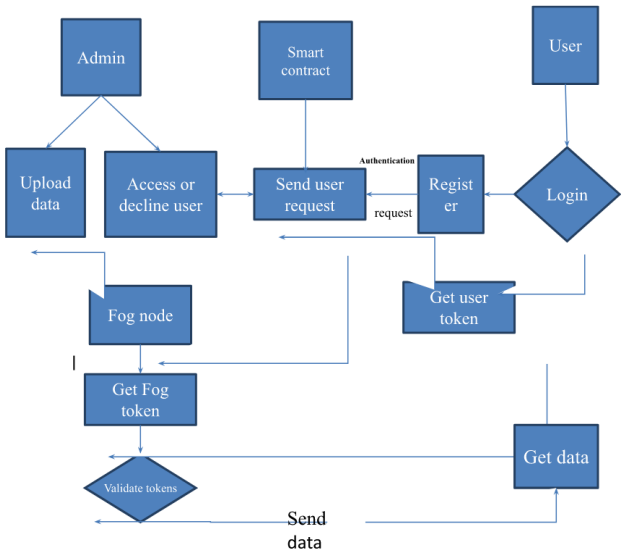

Fig 1: DFD

VI. Technologies

Fog computing is a distributed computing architecture that aims to bring the processing power and storage capacity closer to the data sources, reducing latency and improving data processing speed. The following technologies are used for fog computing:

1. Edge Computing: Edge computing is a computing model that aims to bring computing resources closer to the data sources, reducing the amount of data that needs to be transferred to the cloud for processing. Edge computing is a fundamental technology used for fog computing, as it enables the deployment of computing resources closer to the end-users and data sources.
2. Virtualization: Virtualization is a technology that enables the creation of multiple virtual instances of a single physical resource, such as a server or a storage device. Virtualization is used for fog computing to enable the deployment of virtual instances of computing resources on edge devices, enabling the creation of a distributed computing network.
3. Software-Defined Networking (SDN): Software-defined networking is a network architecture that enables the central management and control of network resources using software-based controllers. SDN is used for fog computing to enable the creation of a highly scalable and flexible network architecture that can dynamically allocate network resources based on the changing demands of the network.
4. Containerization: Containerization is a technology that enables the creation of isolated environments, known as containers, that can run applications and services. Containerization is used for fog computing to enable the deployment of applications and services on edge devices, making it easier to manage and deploy applications across a distributed computing network.
5. Machine Learning: Machine learning is a technology that enables computers to learn from data and improve their performance over time. Machine learning is used for fog computing to enable the creation of intelligent edge devices that can perform data processing and analysis locally, reducing the need to transfer data to the cloud for analysis. This approach can significantly reduce network latency and improve the overall performance of the system.

VI. Methodologies

1. Data Management: Fog computing requires efficient data management methodologies to ensure that data can be stored, processed, and analyzed locally on edge devices. Data management methodologies for fog computing include distributed file systems, data replication, data partitioning, and data aggregation.
2. Resource Management: Resource management methodologies are used to allocate computing resources, such as CPU, memory, and storage capacity, across the distributed computing network. Resource management methodologies for fog computing include load balancing, task scheduling, and resource provisioning.
3. Security and Privacy: Security and privacy are critical concerns for fog computing, as edge devices are often deployed in remote or unsecured locations. Security and privacy methodologies for fog computing include data encryption, access control, intrusion detection, and anomaly detection.
4. Communication Protocols: Fog computing requires efficient communication protocols to enable communication between edge devices and the cloud. Communication protocols for fog computing include MQTT, CoAP, and AMQP.
5. Machine Learning and Artificial Intelligence: Machine learning and artificial intelligence methodologies are used for fog computing to enable the creation of intelligent edge devices that can perform data processing and analysis locally. Machine learning and artificial intelligence methodologies for fog computing include deep learning, neural networks, and decision trees.

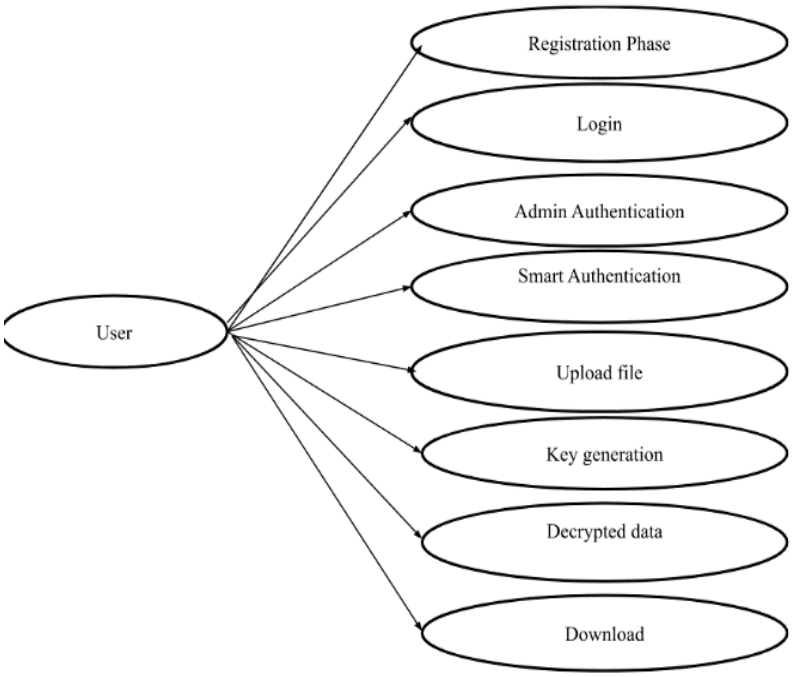

Fig 2: Diagram of uses cases

VII. Modules

User Authentication : User authentication is a process that allows a device to verify the identity of someone who connects to a network resource.

File Upload : Uploading is the transmission of a file from one computer system to another, usually larger computer system.

Key Generation : Key management refers to management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, crypto-shredding (destruction) and replacement of keys.

File Download : Computing services will be able to encrypt documents to keep them safe in the cloud

Admin Acess : Admins are entities responsible for managing he user access control list and permissions for uploaded file.

VIII. Advantages

1. Reduced Latency: By deploying computing resources closer to the data sources, fog computing reduces the time it takes for data to travel from the data source to the cloud for processing and analysis. This reduced latency results in faster data processing and analysis, enabling real-time decision-making and improving the overall performance of applications and services.
2. Improved Bandwidth Efficiency: Fog computing reduces the amount of data that needs to be transferred to the cloud for processing, resulting in improved bandwidth efficiency. This reduction in data transfer also reduces network congestion, improving the overall network performance.
3. Increased Security: Fog computing can provide an additional layer of security to the data processing and analysis process. By processing and analyzing data locally on edge devices, sensitive data can be kept closer to the source, reducing the need to transfer data to the cloud. This approach can help organizations better protect their data from unauthorized access and reduce the risk of data breaches.
4. Scalability: Fog computing is highly scalable, enabling the addition of new edge devices to the network as the volume of data generated by IoT devices and other data sources grows. This scalability enables organizations to handle large volumes of data without requiring expensive centralized data centers.
5. Cost-Effective: Fog computing can be more cost-effective than traditional cloud computing, as it reduces the need for expensive centralized data centers and enables organizations to process and analyze data locally on edge devices. This approach can significantly reduce the costs associated with data transfer and processing, making fog computing a more cost-effective solution.

IX. Conclusion

We have proposed a system design, and implementation of a Block chain-based solution using Ethereum smart contracts for IoT devices authentication at scale, in a decentralized manner with no intermediary third party. We implemented the proposed Ethereum smart contract. Authenticating large scale of IoT devices is featured by involving fog nodes which are used to relieve the IoT devices from the processing burden of carrying out authentication tasks and the connectivity overhead involved with interfacing with the Ethereum Block chain network.

X. Future Scope

- Each IoT node can be registered and authenticated in the blockchain and will have a unique ID and address. Thus, it will help in unique identification of the device. If any device wants to connect with another device, it will use its unique blockchain ID and its local blockchain wallet to raise a request.
- Depending on the IoT device and its network role, IT admins can use other software authentication methods such as digital certificates, organization-based access control and distributed authentication through the Message Queuing Telemetry Transport (MQTT) protocol.
- The collaboration of IoT and Blockchain frameworks will ensure high-security standards for storing and transmitting data between connected cars and IoT platforms. According to a report, it is estimated by 2025, around 10-15% of transactions on connected vehicles will likely be done using blockchain technology.
- Blockchain Reduces the IoT Security and Scalability Vulnerabilities. As discussed above, the IoT is vulnerable to security threats such as ransomware, hacking, data breach, or data tampering. Thus, blockchain is a security solution that will keep the IoT network secured.
- By 2030, it could be used as a foundational technology for 30 per cent of the global customer base. By 2025, blockchain would add a business value that will grow to over $176 billion. This would increase further to $3.1 trillion by 2030. It simply shows the unfolding potential

XI. References

[1] S. Z. Syed Idrus, E. Cherrier, C. Rosenberger, and J.-J. Schwartzmann, "A review on authentication methods," vol. 7, pp. 95–107, 06 2013.

[2] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395 – 411, 2018. [Online]. Available: http://www.sciencedirect. com/science/article/pii/S0167739X17315765 L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," pp. 254–269, 10 2016.

[3] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," CoRR, vol. abs/1802.04410, 2018. [Online]. Available: http://arxiv.org/abs/1802. 04410

[4] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "Iot-oas: An oauth-based authorization service architecture for secure services in iotscenarios," IEEE Sensors Journal, vol. 15, no. 2, pp. 1224–1234, Feb 2015.

[5] Bonomi, F., Milito, R., Natarajan, P., & Zhu, J. (2012). Fog computing: A platform for internet of things and analytics. In Big data and internet of things: A roadmap for smart environments(pp. 169-186). Springer.

[6] Chi, Y., Xu, X., Wang, Y., & Wang, Y. (2019). Research on fog computing: Review, taxonomy, and open research issues. IEEE Internet of Things Journal, 6(2), 2590-2609.

[7] Alrawais, A., Alhothaily, A., Hu, C., Cheng, X., & Hu, F. (2017). Fog computing for sustainable smart cities: A survey. ACM Computing Surveys (CSUR), 50(3), 1-37.

[8] Hwang, I., Jeong, S., & Yoon, Y. (2019). A survey on fog computing: Concepts, applications and issues. Journal of Network and Computer Applications, 128, 82-105.

[9] Varghese, J., &Buyya, R. (2019). Fog computing: Principles, architectures, and applications. In Internet of things (pp. 1-22). Springer.