WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Implementation 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]Project Guide, Information Technology Department, SMT. RadhikataiPandav College of Engineering, Nagpur, India
DOI: https://doi.org/10.55248/gengpi.234.4.38226

ABSTRACT —

The primary goal of this project is to securely store and maintain healthcare data using blockchain technology. By leveraging the security features of blockchain, the healthcare data hosted within the cloud can be protected. Each block contains the data and a timestamp, which allows healthcare providers to securely access IoT data from anywhere.

We propose a user authentication scheme that uses blockchain-enabled fog nodes. These fog nodes interface with Ethereum smart contracts to authenticate users who want to access IoT devices. Blockchain is a decentralized, distributed, shared, and immutable database ledger that stores a registry of assets and transactions across a peer-to-peer (P2P) network. It ensures that the data is preserved from attackers.

Before outsourcing the data to the cloud, it is encrypted to ensure its privacy. The healthcare provider must decrypt the data before downloading it.

Keywords — IoT, Cisco, File storage, file management, Fogg computing, Secure Storage, Healthcare.

I. Introduction

The deployment of IoT devices is rapidly increasing, with Cisco forecasting 20 billion devices by 2020. These devices are resource-constrained, making them vulnerable to hacking and compromise. It is therefore essential to implement proper authentication and access control schemes to ensure the security of IoT devices, their communications, and their data. However, any authentication scheme for IoT devices must consider their limitations in processing and computation, and should be reliable, scalable, and secure against known attacks and threats.

Fog computing has emerged as a promising computing paradigm that can perform localized processing, storage, and analytics for groups of IoT devices, relieving them of some of their heavy computational workloads. Blockchain technology is also being explored as a viable solution to the challenging security issues faced by IoT devices. However, most authentication techniques for IoT systems are centralized, relying on a Trusted Third Party, which is costly and vulnerable to hacking and privacy evasion.

To address the limitations of centralized authentication, this paper proposes a decentralized authentication scheme using fog nodes and blockchain technology. The scheme facilitates managing and accessing IoT devices while providing security without the need for a Trusted Third Party. The proposed architecture involves end users, IoT devices, fog and cloud nodes, and Ethereum Blockchain smart contracts that govern the authentication rules and logic. The proposed work also involves the use of new architectures, such as edge computing and blockchain, which facilitate authentication at scale.

The primary contribution of this paper is the proposal and analysis of the security of a blockchain-based authentication scheme for IoT devices. Specifically, the paper presents 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. Access tokens are issued by the smart contracts with no intermediary or trusted third party involved.

II. Problem Statement

To address these challenges, many organizations are turning to edge computing solutions. Edge computing refers to the use of decentralized computing resources, located closer to the data source, to process and store data. This approach offers several benefits over traditional cloud computing solutions, including reduced latency, improved data privacy and security, and better scalability.

With edge computing, organizations can process data in real-time, reducing the need for data to be transferred to a centralized location for processing. This approach not only improves data processing speed, but it also reduces the risk of data breaches, as sensitive data is not transmitted over long distances. Additionally, edge computing solutions are more resilient to network outages and can operate autonomously, even when disconnected from the network.

Another advantage of edge computing is that it can help organizations manage data from multiple locations and devices. By deploying edge computing resources in various locations, organizations can process and store data from different devices and locations, without relying on a centralized file management system. This approach enables faster data processing and improves overall data management efficiency.

In summary, as data generation and storage needs continue to grow, traditional cloud computing solutions may not be able to keep up with the pace of data processing and storage requirements. Edge computing solutions offer a more decentralized approach to data processing and storage, providing several benefits, including improved speed, data privacy and security, scalability, and efficient data management.

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. Improved Performance: One of the main objectives of fog computing is to improve the performance of distributed systems and applications by bringing computing and storage resources closer to the edge of the network. This reduces latency and network congestion, resulting in faster data processing and response times.
2. Reduced Bandwidth Consumption: Fog computing aims to reduce the amount of data that needs to be transmitted to the cloud by performing data processing and analysis locally. This reduces the bandwidth consumption of the network and enables real-time decision making.
3. Enhanced Security: Another objective of fog computing is to enhance the security and privacy of data by keeping sensitive information closer to the edge of the network and reducing the number of data transfers to the cloud. This helps to minimize the risk of data breaches and cyber attacks.
4. Scalability: Fog computing aims to provide a scalable computing architecture that can handle a large number of devices and applications in a distributed environment. By distributing computing resources across the network, fog computing can improve the scalability of applications and services.
5. Lower Costs: By reducing the amount of data transmitted to the cloud, fog computing can reduce the costs associated with network bandwidth and cloud computing. This makes fog computing an attractive option for organizations that need to process and analyze large amounts of data in real-time, without incurring high costs.

IV. LITERATURE SURVEY

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 leakage

E. 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 leakssignificantlylessinformation 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
- Efficient no-dictionary verifiable SSE

W. Ogata and K. Kurosawa

A generic method to transform any SSE scheme (that is only secure against passive adversaries) to a no-dictionary verifiable SSE scheme. A client encrypts a set of files and an index table by a symmetric encryption scheme, and then storesthem on an untrusted server. In the search phase, he can efficiently retrievethe matching files for a search keyword w keeping the keyword and the files secret.

Advantage:

- ✔ Efficient data search

Disadvantage:

- ✔ Data Integrity Problem
- Parallel and Dynamic Searchable Symmetric Encryption

S. Kamara and C. Papamanthou

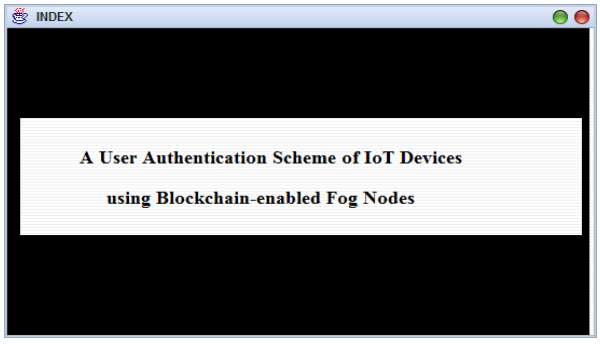
Searchable symmetric encryption (SSE) enables a client to outsource a collection of encrypted documents in the cloud and retain the ability to perform keyword searches without revealing information about the contents of the documents and queries. Although efficient SSE constructions are known, previous solutions are highly sequential. This is mainly due to the fact that, currently, the only method for achieving sub-linear time search is the inverted index approach

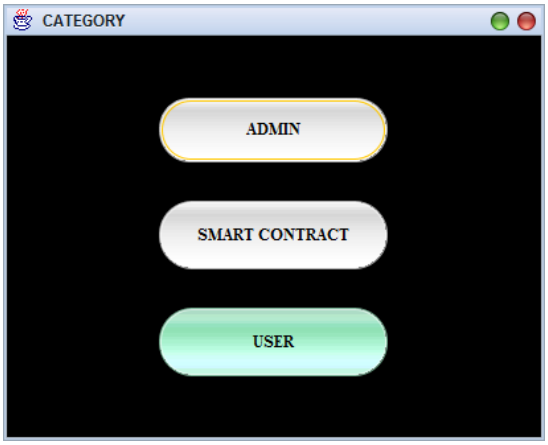
Efficient data management

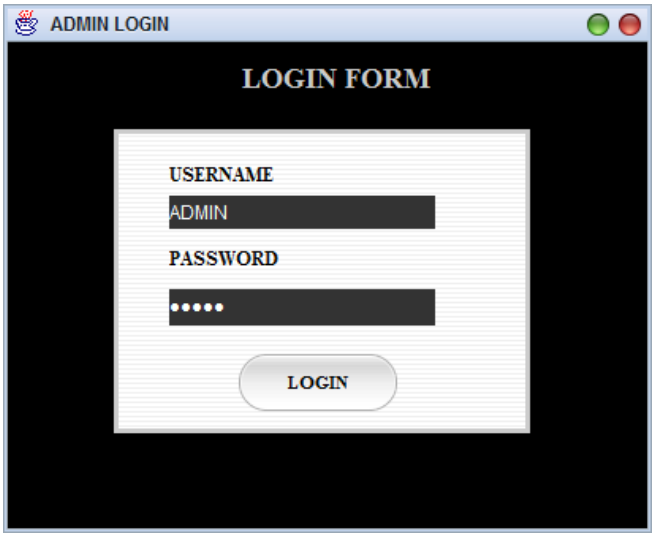
Disadvantages:

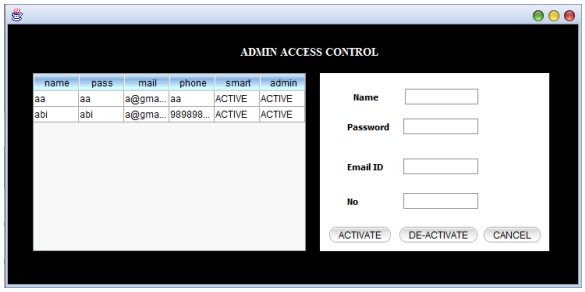
Privacy Issues.

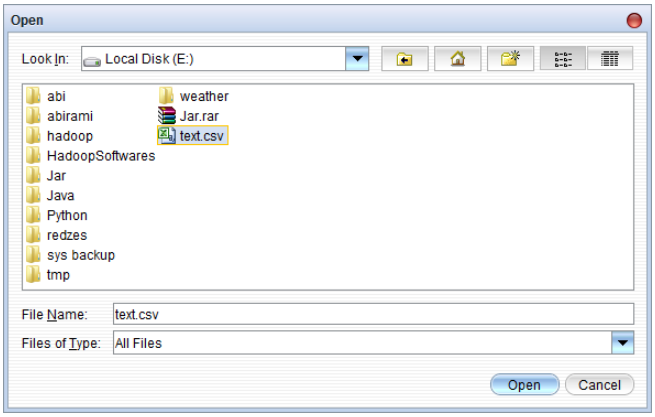
V. Screenshots

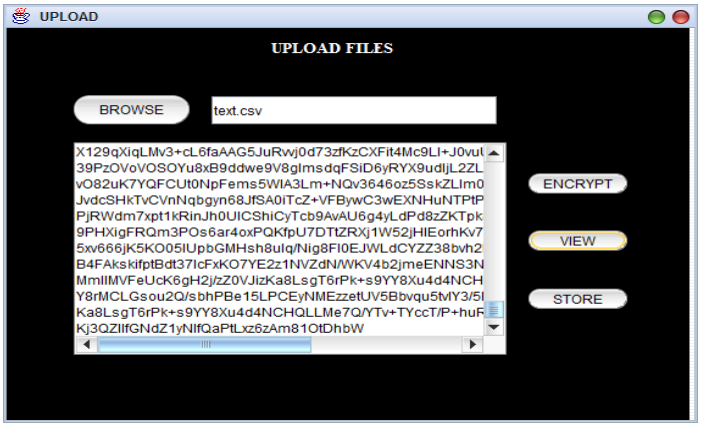





ADMIN LOGIN
LOGIN FORM
USERNAME
ADMIN
PASSWORD
LOGIN


ADMIN ACCESS CONTROL
name
pass
mail
phone
smart
admin
aa
aa
a@gma...
aa
ACTIVE
ACTIVE
abi
abi
a@gma...
989898...
ACTIVE
ACTIVE
Name
Password
Email ID
No
ACTIVATE
DE-ACTIVATE
CANCEL


Open
Look In:
Local Disk (E:)
abi
abirami
hadoop
HadoopSoftwares
Jar
Java
Python
redzes
sys backup
tmp
weather
Jar.rar
text.csv
File Name:
text.csv
Files of Type:
All Files
Open
Cancel


UPLOAD
UPLOAD FILES
BROWSE
text.csv
ENCRYPT
VIEW
STORE

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.

VII. 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.

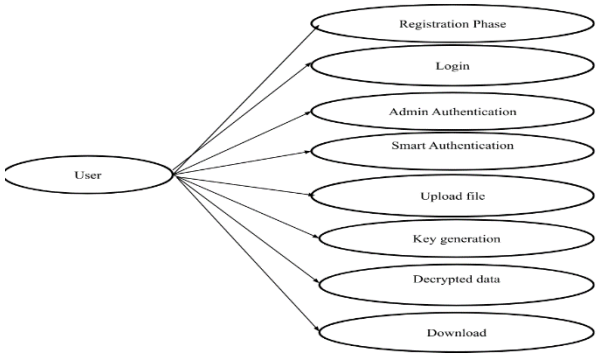


Fig 2: Diagram of uses cases

VIII. 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.

IX. 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.

X. 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.

XI. 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

XII. References

[1] Zhang, Y., Wen, Y., Wu, Z., & Zhang, D. (2018). An overview of fog computing and its security issues. Journal of Network and Computer Applications, 98, 27-42.

[2] Kumar, A., Prakash, S., & Singh, S. (2018). A systematic review on fog computing: Concepts, architecture, and applications. Journal of Network and Computer Applications, 108, 13-42

[3] Mukherjee, A., Ghosh, A., Datta, S., & Chatterjee, J. (2019). Fog computing: Vision, challenges, and research directions. Journal of Ambient Intelligence and Humanized Computing, 10(8), 3049-3070.

[4] Li, J., Li, Y., Li, X., Li, J., & Yang, Y. (2019). Fog computing for the internet of things: A survey. IEEE Internet of Things Journal, 6(3), 4794-4811.

[5] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

[6] Hsu, C. H., Liao, Y. H., & Tsai, C. W. (2018). Fog computing in healthcare internet of things: A review of the emerging trends and paves the way for future research directions. Journal of Ambient Intelligence and Humanized Computing, 9(6), 2205-2220.

[7] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637-646.

[8] Aazam, M., Zeadally, S., &Harras, K. A. (2018). Fog computing architecture for big data and IoT: A survey. IEEE Communications Magazine, 56(2), 94-100.

[9] Bonomi, F., Milito, R., Zhu, J., &Addepalli, S. (2012). Fog computing and its role in the internet of things. In Proceedings of the first edition of the MCC workshop on mobile cloud computing (pp. 13-16).

[10] Calheiros, R. N., Ranjan, R., Beloglazov, A., De Rose, C. A., &Buyya, R. (2015). CloudSim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. Software: Practice and Experience, 45(1), 1-31.