

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 3, May-June 2025

Impact Factor: 8.152



Effective Identity Authentication Based on Multi Attribute Centers for Secure Government Data Sharing

Shaikh Mohamad¹, Sai Aditya Prasad², Sri Harsha Jasti³, Cheethirala Thrinadh⁴

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India¹

Student, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India²⁻⁴

ABSTRACT: Identity authentication is an essential part of ensuring secure data exchange within government systems, particularly when working with large amounts of data. Traditional approaches that rely on a single trusted authority can lead to issues like information leaks, dependence on a central point that might fail, and concerns over key escrow. To overcome these drawbacks, this work introduces a new identity authentication method based on several attribute centers. Each center provides a private key linked to a specific attribute of the data requester. Once all the relevant keys are obtained, the requester can use them to create a personal private key.. Second, a dynamic key generation technique is suggested that uses smart contracts and blockchain technology to refresh a data requester's key on a regular basis. This lowers the chance of privacy leaks, ensures IA traceability, and guards against theft by outside attackers. Third, to further lower the cost of blockchain information storage and increase its efficacy, attribute field information of the data requester is stored using a mix of blockchain technology and interplanetary file systems. According to experimental data, the suggested approach outperforms comparable authentication models in terms of communication and computing costs while guaranteeing the privacy and security of identity information.

I.INTRODUCTION

With the rise of the information era, data has become a valuable asset, driving advancements across various sectors. For government agencies, one of the shared objectives is to enhance collaboration by promoting data exchange across departments and moving toward a smarter, service-driven digital government. However, this goal is often hindered by fragmented data storage across departments, weak security measures for shared data, and the lack of a reliable way to verify the identity of those accessing the information. Another major challenge in government data sharing is the difficulty of assigning clear accountability for the data, which makes full and open sharing difficult to achieve. As a result, there is a growing need for a secure and efficient solution to support interdepartmental data exchange. Identity Authentication (IA) serves as the foundational step in securing the sharing of government data across departments. Effective security and privacy controls are essential to prevent unauthorized access and misuse of sensitive information. Traditional authentication models often depend on third-party trust systems—such as Public Key Infrastructure (PKI), cloud-based certificate authorities, and internet address management protocols—which come with their own limitations. A typical IA framework includes three core entities: the data requester, the authorization center, and the data owner. In this setup, the requester first registers their identity with the authorization center. When access to data is needed, a request is sent to the data owner, who confirms the requester's identity through the authorization center. Conventional password-based methods are inexpensive and easy to implement, as they rely solely on passwords without additional hardware or software requirements. However, these approaches are increasingly susceptible to network threats and provide limited protection. This highlights the need for stronger, multifactor authentication strategies. In traditional centralized IA systems, control lies with the central authority, not the users. This means users must place full trust in the authority, which not only manages their keys but also creates the risk of key escrow. Moreover, such centralized control can introduce a critical vulnerability: if the central authority fails, the entire authentication system may collapse due to a single point of failure.

II.LITERATURE SURVEY

Traditional authentication methods generally depend on trust established by third-party entities, including well-known systems like Public Key Infrastructure (PKI), cloud-based trusted certificate authorities, and current internet address allocation frameworks. A typical identity authentication (IA) model, as illustrated involves three key participants: the data requester, the authorization center, and the data owner. Initially, the data requester registers their identity with the

authorization center. Later, when data access is needed, the requester sends a request to the data owner, who then confirms the requester's identity through the authorization center.

Title: Correlation graph based approach for personalized and compatible web APIs recommendation in mobile APP development

Year: 2023

Author: L. Qi, W. Lin, X. Zhang, W. Dou, X. Xu and J. Chen,

Description

Using Web APIs from service-sharing platforms can speed up mobile app development and cut costs while keeping apps current by reusing advanced features. However, choosing the right APIs is challenging due to their variety and compatibility issues.

To address this, we construct a correlation graph that links API functions with compatibility data. Based on this graph, we propose a personalized recommendation method to suggest APIs that meet both functional and compatibility needs. Tests on real-world data confirm the approach's effectiveness.

Title: Path planning for energy management of smart maritime electric vehicles: A blockchain-based solution

Year: 2023

Author: A. Barnawi, S. Aggarwal, N. Kumar, D. M. Alghazzawi, B. Alzahrani and M. Boulares

Description

Vehicle-to-grid (V2G) technology is used in the modern eco-friendly environment for demand response management. Reducing carbon emissions is one of the key benefits of using electric vehicles. However, when data is shared over open networks like the Internet—especially between entities such as plug-in hybrid electric vehicles (PHEVs), charging stations (CSs), and controllers in a Vehicle-to-Grid (V2G) setup—security and privacy become major concerns. As electric vehicle (EV) adoption grows rapidly worldwide, there is a growing need for reliable and secure charging and billing systems. To address this, we propose a blockchain-based demand response system that enables secure and efficient energy trading between EVs and charging stations. In our approach, miner nodes and block verifiers are chosen based on their energy usage and computing power. These nodes handle transaction authentication within the system. We also introduce a game theory-based strategy to manage energy use and control peak loads during high and low demand periods. Our proposed method has been tested using standard performance metrics, and the results show it performs better than existing approaches.

Title: Blockchain-based architecture centred patient for decentralised storage and secure sharing health data

Year: 2022

Author: K. Zarour, O. A. Bounab, Y. Marir and I. Boumezbeur

Description

Data-sharing systems between patients and healthcare providers have improved medical services and supported research. However, these advances raise serious data security concerns. Traditional centralized storage methods are increasingly vulnerable, especially with the rise of portable devices. To address this, we propose a secure and decentralized healthcare data-sharing system using Blockchain and the InterPlanetary File System (IPFS).

Title: Survey of authentication in internet of things-enabled healthcare systems

Year: 2022

Author: M. A. Khan, I. U. Din, T. Majali and B. S Kim

Description

The Internet of Medical Things (IoMT) connects people, devices, sensors, and systems to enhance healthcare using modern technology. Over time, several systems have been developed to make the most of IoMT, aiming to make healthcare more efficient, accessible, and secure through the use of IoT. Despite the benefits of location- and time-independent health services, the shift to IoT-based healthcare has also brought many new challenges. One of the main concerns is system security, especially the process of authentication, which ensures that users, devices, or systems are properly identified before gaining access. This survey reviews various authentication methods used in IoT-based healthcare environments. It organizes the discussion based on where the technology is implemented—cloud, fog, or edge computing. The paper also includes a classification of potential attacks, a detailed review of current authentication strategies, and suggestions for future research in this area.

Title: A new distributed decentralized privacy-preserving ID registration system

Year: 2021

Author: J. S. Shin, S. Lee, S. Choi, M. Jo and S. H. Lee

Description

Blockchain, widely known as a distributed ledger, is now being used in key areas like smart grids to improve privacy and security. Some systems have introduced privacy-preserving methods that ensure data integrity and user anonymity. Earlier approaches relied on Bloom filters and centralized key management, but they lacked full decentralization and couldn't handle key updates or revocation effectively.

To address these issues, this work proposes a fully decentralized identity scheme. It uses blind signatures to maintain user anonymity and advanced Bloom filters for managing key updates and revocations. A distributed certification authority handles key management, eliminating the need for a central authority. This approach is suitable not only for smart grids but also for sectors like banking, healthcare, and digital public services such as e-voting and online surveys.

III.EXISTING SYSTEM

Relying on a centralized identity authentication system that depends on a single trusted party can lead to several risks, including potential data leaks, vulnerabilities from a single point of failure, and complications related to key escrow. To address these challenges, this paper proposes a more resilient identity authentication model that distributes responsibilities across multiple attribute authorities. However, the efficiency of government data sharing is significantly affected because of data storage in separate departments, low security of shared information storage, and uncertainty of the sharer's identity. Furthermore, it is difficult to assign responsibility for government data, which makes it challenging to share the data fully. Therefore, a secure and efficient government data-sharing solution is urgently needed.

EXISTING SYSTEM DISADVANTAGES

- Low security of shared information storage.
- Data storage in separate departments.
- Less efficiency of government data sharing

IV.PROPOSED SYSTEM

To begin with, the attribute authorization center issues a private key for each specific attribute associated with the data requester. Once these keys are obtained, the requester uses them to generate their own personal private key. Second, a dynamic key generation algorithm is proposed, which combines blockchain and smart contracts to periodically update the key of a data requester to prevent theft by external attackers, ensure the traceability of IA, and reduce the risk of privacy leakage. Third, the combination of blockchain and interplanetary file systems is used to store attribute field information of the data requester to further reduce the cost of blockchain information storage and improve the effectiveness of information storage.

PROPOSED SYSTEM ADVANTAGES

- More security of shared information storage.
- Data storage in server departments.
- Effectiveness of government data sharing

V.SYSTEM ARCHITECTURE

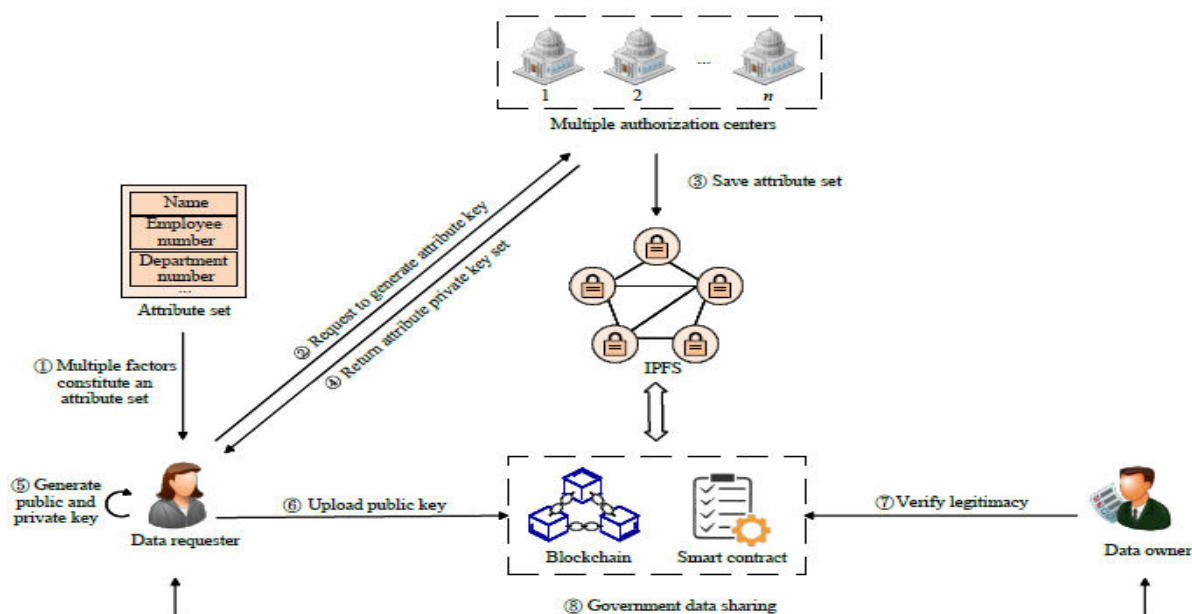


Fig: System Architecture Model

Smart contract: This program is combined with blockchain technology to manage the time validity of the data requester's keys.

IPFS: It stores the attribute information of the data requester and uses the hash function to calculate a unique hash value for each attribute. IPFS is combined with blockchain to store identity information, ensure data security, and reduce storage costs.

Authorization center: The proposed scheme employs multiple attribute authorization centers that are responsible for generating corresponding attribute keys for the data requester.

Government data sharing: The data owner shares their information with the data requester, who uses the information to meet the department's needs.

The system architecture is divided into the following components:

- **User Interface Design**
- **Data Owner**
- **Third Party Authorization Center**
- **Data Requester/Consumer**

VI.METHODOLOGY

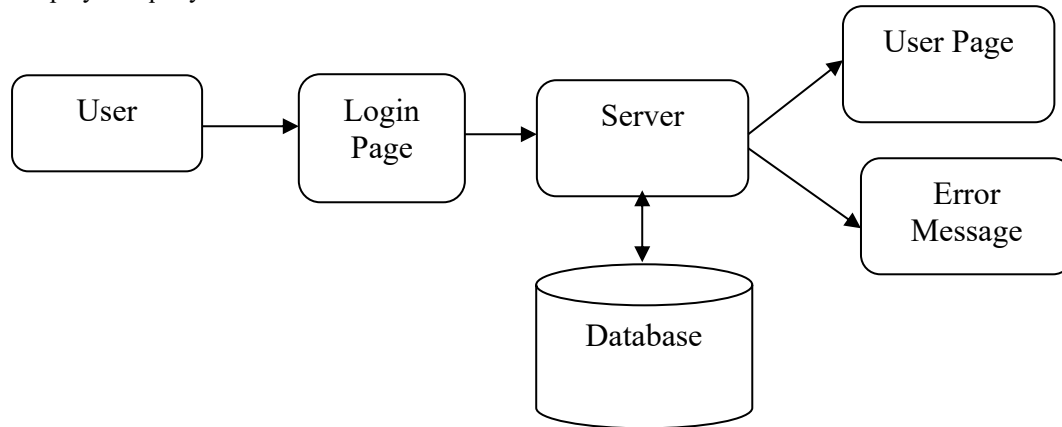
MODULES NAMES

- User Interface Design
- Data Owner
- Third Party Authorization Center
- Data Requester

1.User Interface Design

To connect with server user must give their username and password then only they can able to connect the server. If the user already exists directly can login into the server else, user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and

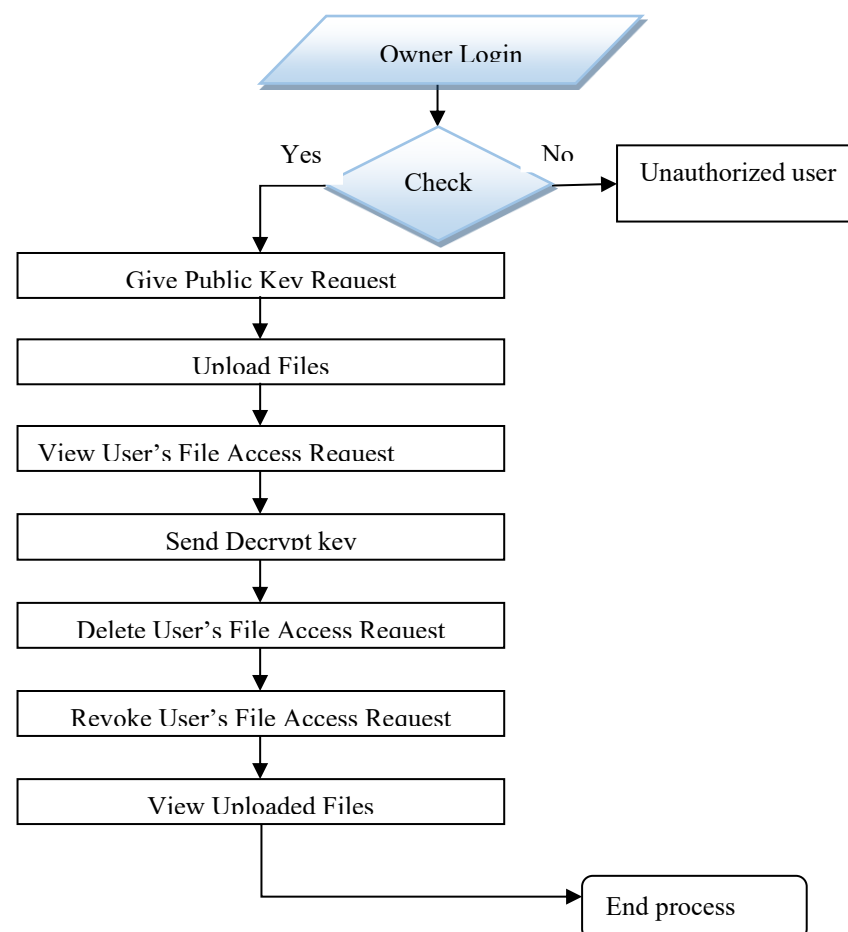
download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.



2.Data Owner

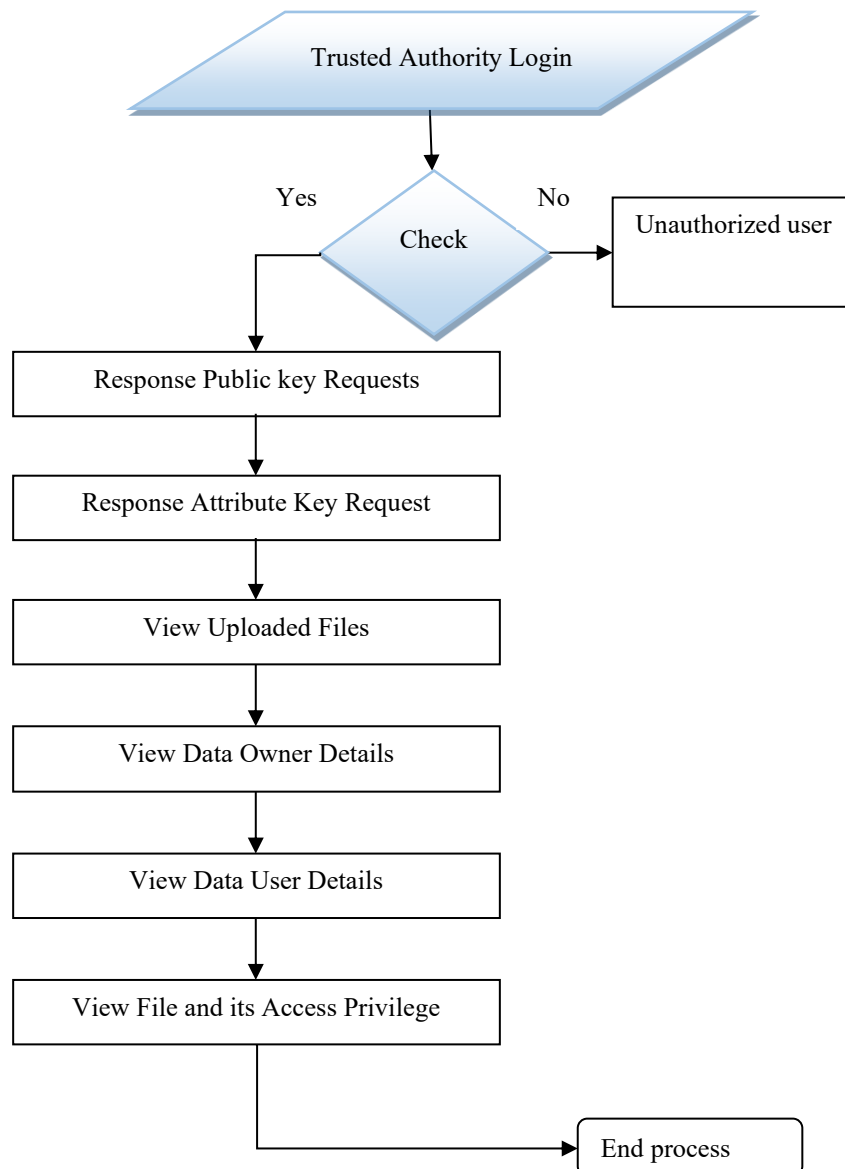
The data owner verifies the legitimacy of the data requester through the blockchain. Storing data in the blockchain incurs transaction costs and therefore is unsuitable for storing large amounts of data. Accordingly, we store hash values of data in the system for cost reduction. Finally, the data owner verifies the legitimacy of the data requester's identity through the IA scheme based on blockchain and NIZKP.

Government data sharing: The data owner shares their information with the data requester, who uses the information to meet the department's needs.



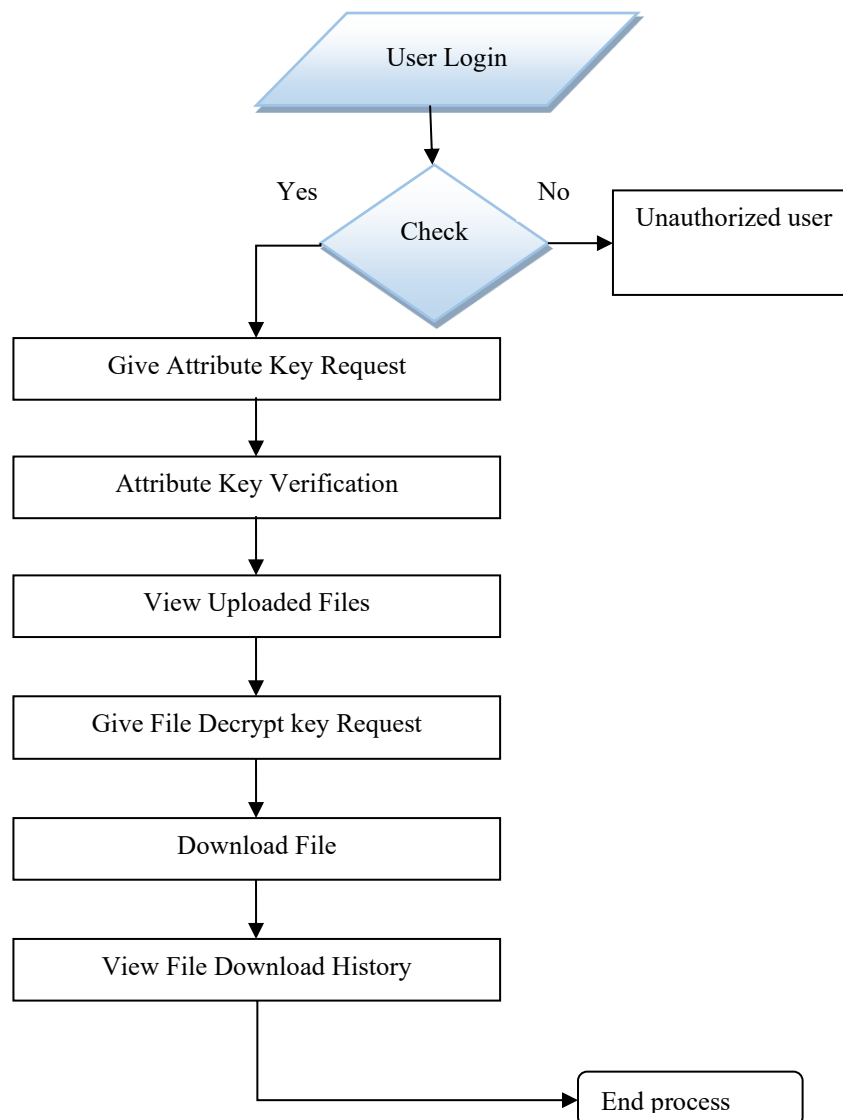
3.Third Party Authorization Center

A trusted authority controls the user's keys, which may lead to potential key escrow. Such a highly centralized feature can render the whole system unable to operate and cause a risk of a single point of failure in case the authority fails. The proposed scheme employs multiple attribute authorization centers that are responsible for generating corresponding attribute keys for the data requester. **Attribute set:** The data requester composes an attribute set according to multiattribute factors such as name, employee number, and department number, which are used to generate attribute keys to address the issue of inflexible single-factor authentication.



4.Data Consumer

The person in charge of a governmental department who provides data to other departments. The data owner is responsible for verifying the legitimacy of the data requester's identity, which is assumed to be trustworthy in this study. The person in charge of a governmental department who requests access to the data of other departments. The data requester can query the appropriate data owner through a smart contract and prove the legitimacy of his/her identity and then request the corresponding access. The proposed scheme employs multiple attribute authorization centers that are responsible for generating corresponding attribute keys for the data requester.



VII. ALGORITHMS USED

Dynamic Key Generation

Thus, the private key $du=(d_0, d_1)$ of each attribute $j \in I'$ is obtained. After obtaining the private key for each attribute, the data requester generates a personal private key K_u . At the same time, the elliptic curve is used to calculate $Qu=KuG'$ to generate its public key $Qu, Qu \in E(F_p)$, where $E(F_p)$ represents the elliptic curve E defined over the finite field F_p , and G' is a generator of the elliptic curve E . The data requester uploads the public key information to the blockchain. To prevent the private key of the data requester from being stolen by the attacker, a dynamic key generation algorithm is designed, as shown in Algorithm 1.

In the dynamic key generation algorithm, the concept of delay time is introduced, which is recorded as D_t , and in this algorithm, we define a smart contract. The delay time D_t is equivalent to the validity period of the public key. The smart contract records the public key Q_u and the delay time D_t of the data requester, which is recorded as $Y=\{Q_u,D_t\}$. $R=(0,1)$ represents the result of IA, where 1 represents that the public key is valid, 0 otherwise.

When the set time comes, the smart contract automatically executes an operation to revoke the public key without human intervention, thereby making it invalid. Specifically, after D_t , the smart contract automatically deletes Y , indicating that the public key of the data requester is invalid. Deleting a public key does not actually modify the data within the block in the blockchain, but rather indicates that Y has been invalidated by initiating a new transaction. The underlying blockchain retains historical information, which is publicly accessible. Once the data owner queries the blockchain for Y invalid transactions, the data requester cannot be authenticated, and needs to re-execute the key generation phase to prevent external attackers from stealing the key. Even if a malicious attacker succeeds in stealing the data requester's private key, the intercepted information is unusable after the key is dynamically changed. Thus, the loss of the data requester is minimal.

VIII. EXPERIMENTAL RESULTS




Fig : Home Screen(Landing Page)




Fig: Data Owner Section

DATA OWNER REGISTRATION



Name
 Password
 Mail

Choose Gender 



 Gender
 dd-mm-yyyy  DOB
 Contact Number
 State
 Country

Fig: Data Owner Registration


DATA OWNER LOGIN



Username
 Password

Fig: Data Owner Login

DATA OWNER HOME



Menu Bar

- Home
- Public Key Request
- Upload File
- View Data User File Access Request
- View Uploaded Files
- Logout

When the data owner (DO) registers on TA, TA runs the algorithm Setup() to generate a public key PK and a master key MK. PK is sent to DO while MK is kept on TA itself. Data Owner uploads data to the mobile cloud and share it with friends. The cloud is not credible, data has to be encrypted before it is uploaded. DO determines the access control policies.

Fig: Data Owner Landing Page

Public Key Request

Id	Name	Mail	Status	Give Request
5	owner6	owner6@gmail.com	Give Request	Request


Note: If Status is Waiting means your request sent to TA but TA not yet Generate a Public key
 Note: If Status is Update means you can Update your Public key

Menu Bar

- Home
- Public Key Request
- Upload File
- View Data User File Access Request
- View Uploaded Files
- Logout

Fig: Data Owner Requesting Public Key

TRUSTED AUTHORITY LOGIN




Username

Password

Fig: Trusted Authority Login

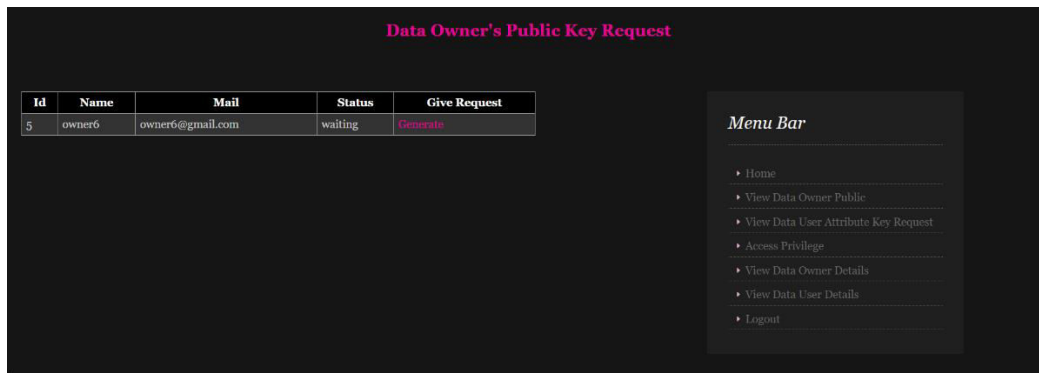
TRUSTED AUTHORITY HOME



Menu Bar

- Home
- View Data Owner Public Key Request
- View Data User Attribute Key Request
- View Data Owner Details
- View Data User Details
- Access Privilege
- Logout

Fig: Trusted Authority Home Screen After Login

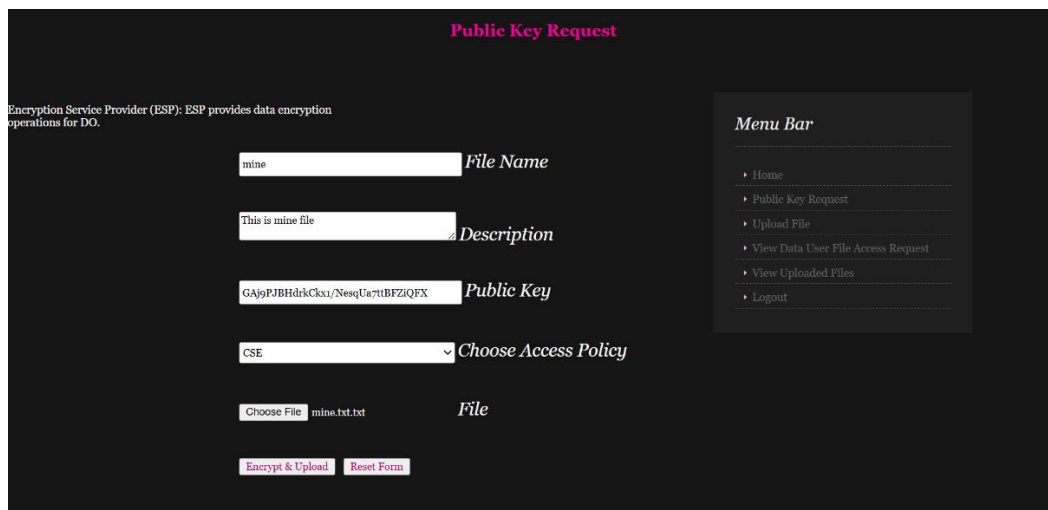


Id	Name	Mail	Status	Give Request
5	owner6	owner6@gmail.com	waiting	Generate

Menu Bar

- Home
- View Data Owner Public
- View Data User Attribute Key Request
- Access Privilege
- View Data Owner Details
- View Data User Details
- Logout

Fig: Data Owner's Public Key Request



Encryption Service Provider (ESP): ESP provides data encryption operations for DO.

File Name:

Description:

Public Key:

Choose Access Policy:

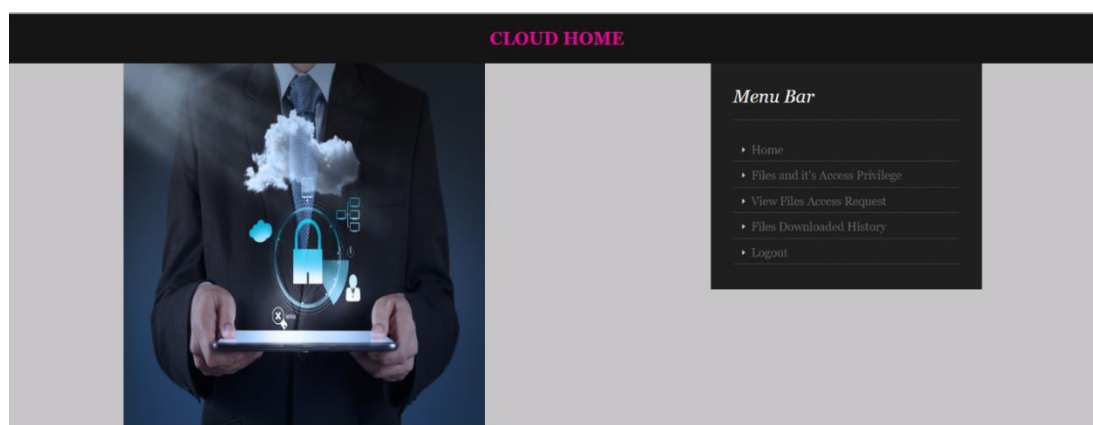
File:

[Encrypt & Upload](#) [Reset Form](#)

Menu Bar

- Home
- Public Key Request
- Upload File
- View Data User File Access Request
- View Uploaded Files
- Logout

Fig: Public Key Request



Menu Bar

- Home
- Files and it's Access Privilege
- View Files Access Request
- Files Downloaded History
- Logout

Fig: Cloud Home Screen After Login

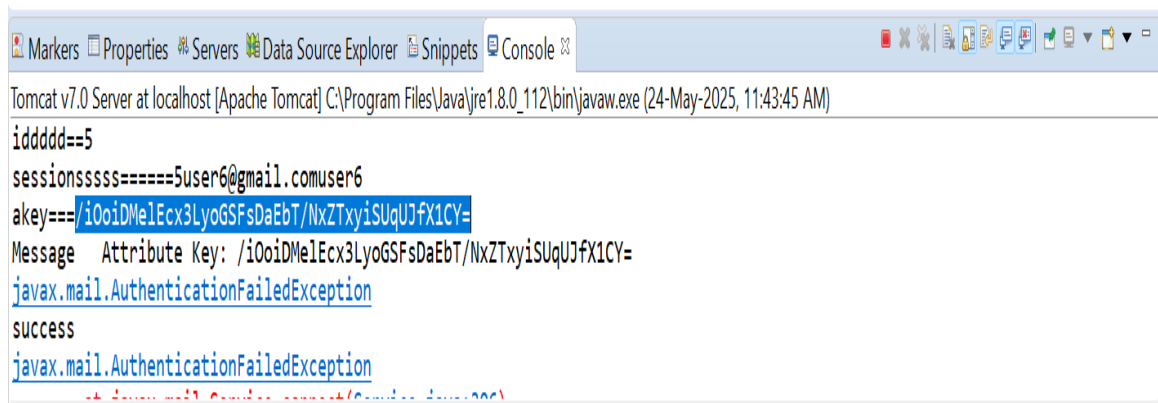


Fig: Encryption Key

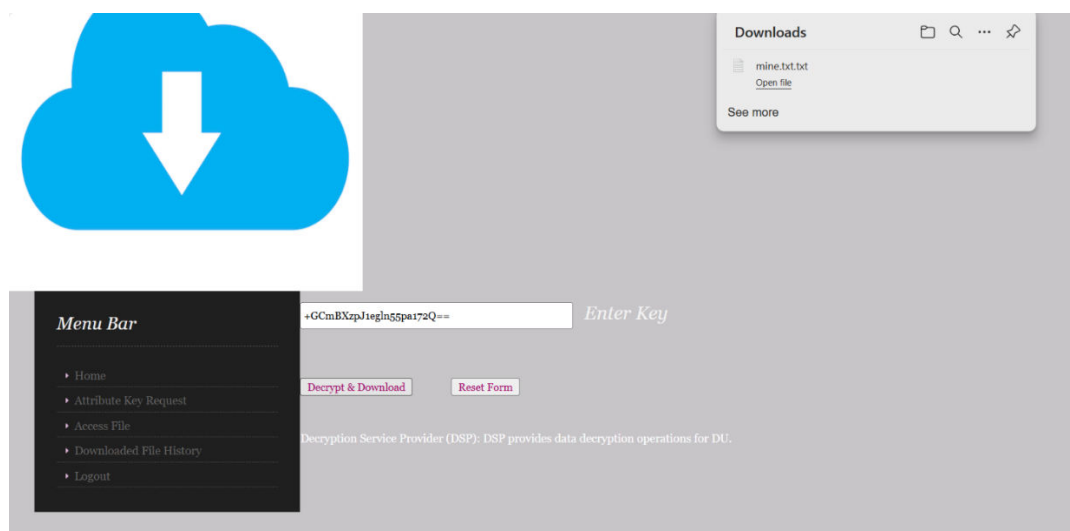


Fig: Decryption Key Entered to Know the Text That Is Sent from One End to Other

IX.CONCLUSION

In this study, the identity legitimacy of government data requesters was considered to ensure the security of data sharing among governmental departments. We propose an efficient IA scheme based on multi-attribute authorization centers. In this scheme, although the data requester needs to spend a certain amount of time to generate a personal private key, the key escrow problem can be solved, and security can be ensured. Further, a dynamic key generation algorithm is proposed wherein the public key of the data requester is configured to be dynamically updated, and the authentication mechanism is deployed through NIZKP. Simulation experiments demonstrated the effectiveness of the proposed scheme. Compared with similar authentication schemes, the proposed scheme performs better in terms of computational and communication costs. However, due to length limitation, there are other issues worth delving into, such as the existence of malicious nodes in blockchain may lead to consensus security problems and how to share data in the next step.

X.FUTURE ENHANCEMENT

Therefore, our future research will focus on designing a reasonable reward and punishment mechanism for nodes to improve consensus efficiency and formulate an efficient and secure data-sharing scheme. This will help maintain the legal integrity of the system and safeguard citizens' data privacy rights during government data sharing. These future enhancements will help strengthen the system's security, scalability, and flexibility, ensuring that it can handle the complexities and challenges of modern government data sharing in a secure, efficient, and user-friendly manner.

REFERENCES

1. L. Qi, W. Lin, X. Zhang, W. Dou, X. Xu and J. Chen, "A correlation graph based approach for personalized and compatible web APIs recommendation in mobile APP development", IEEE Trans. Knowl. Data Eng., vol. 35, no. 6, pp. 5444-5457, 2023.
2. A. Barnawi, S. Aggarwal, N. Kumar, D. M. Alghazzawi, B. Alzahrani and M. Boulares, "Path planning for energy management of smart maritime electric vehicles: A blockchain-based solution", IEEE Trans. Intell. Transp. Syst., vol. 24, no. 2, pp. 2282-2295, 2023.
3. X. Zhou, W. Liang, W. Li, K. Yan, S. Shimizu and K. I. K. Wang, "Hierarchical adversarial attacks against graph-neural-network-based IoT network intrusion detection system", IEEE Internet Things J., vol. 9, no. 12, pp. 9310-9319, 2022.
4. M. A. Khan, I. U. Din, T. Majali and B. S Kim, "A survey of authentication in internet of things-enabled healthcare systems", Sensors, vol. 22, no. 23, pp. 9089, 2022.
5. K. Zarour, O. A. Bounab, Y. Marir and I. Boumezbeur, "Blockchain-based architecture centred patient for decentralised storage and secure sharing health data", Int. J. Electron. Healthcare., vol. 12, no. 2, pp. 170-190, 2022.
6. H. Chai, S. Leng, J. He, K. Zhang and B. Cheng, "Cyber Chain: Cybertwin empowered blockchain for lightweight and privacy-preserving authentication in internet of vehicles", IEEE Trans. Veh. Technol., vol. 71, no. 5, pp. 4620-4631, 2022.
7. J. A. Fernandez-Carrasco, T. Egues-Arregui, F. Zola and R. Orduna-Urrutia, "ChronoEOS: Configuration control system based on EOSIO blockchain for on-running forensic analysis", Proc. Int. Congress on Blockchain and Applications, pp. 37-47, 2022.
8. G. Li, X. Ren, J. Wu, W. Ji, H. Yu, J. Cao, et al., "Blockchain-based mobile edge computing system", Inf. Sci., vol. 561, pp. 70-80, 2021.
9. Z. Rahman, I. Khalil, X. Yi and M. Atiquzzaman, "Blockchain-based security framework for a critical industry 4.0 cyber-physical system", IEEE Commun. Mag., vol. 59, no. 5, pp. 128-134, 2021.
10. M. Di, G. Galatro, M. Longo, F. Postiglione and M. Tambasco, "HASFC: A MANO-compliant framework for availability management of service chains", IEEE Commun. Mag., vol. 59, no. 6, pp. 52-58, 2021.
11. P. Zhang, M. Zhou, Q. Zhao, A. Abusorrah and O. O. Bamasag, "A performance-optimized consensus mechanism for consortium blockchains consisting of trust-varying nodes", IEEE Trans. Netw. Sci. Eng., vol. 8, no. 3, pp. 2147-2159, 2021.
12. Y. M. Tseng, J. L. Chen and S. S. Huang, "A lightweight leakage-resilient identity-based mutual authentication and key exchange protocol for resource-limited devices", Comput. Networks, vol. 196, pp. 108246, 2021.
13. J. Arm, P. Fiedler and O. Bastan, "Offline access to a vehicle via PKI-based authentication", Proc. Int. Conf. on Computer Safety Reliability and Security, pp. 76-88, 2021.
14. W. Wang, H. Huang, L. Zhang, Z. Han, C. Qiu and C. Su, "Block SLAP: Blockchain-based secure and lightweight authentication protocol for smart grid", Proc. IEEE 19 th Int. Conf. on Trust Security and Privacy in Computing and Communications (TrustCom) , pp. 1332-1338, 2020.
15. H. Qiu, M. Qiu and R. Lu, "Secure V2X communication network based on intelligent PKI and edge computing", IEEE Network, vol. 34, no. 2, pp. 172-178, 2020.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975

Impact Factor: 8.152