

Achieving Decentralized and Dynamic SSO-Identity Access Management System for Multi-Application Outsourced in Cloud

G. Lakpathi

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

ABSTRACT: The majority of Single Sign-On (SSO) access control systems in use today rely on traditional protocols that require additional identity providers and/or authentication methods. The increasing requirement to outsource system resources, like data and apps, to cloud platforms makes it impractical to deploy traditional SSO methodologies to provide efficient and granular access control for multi-user and multi-application settings. In this study, we provide D2-IAM, a block chain-based identity and access management (IAM) scheme, as a strong security measure for controlling SSO access to cloud resources. Essentially, smart contracts and blockchain technology are used in D2-IAM's access control processes, and every access transaction is meticulously documented for accountability. Our system's SSO authentication is based on the highest level of authentication and hashed-based token management. Because of the autonomous authentication management, there is less communication overhead when working with identity providers and third-party verification mechanisms for multi-system authentication. D2-IAM uses access policies that are specified, upheld, and represented for each client in the document database to give granular access to the authorization system.

I. INTRODUCTION

Access control, crucial for information systems, includes authentication, authorization, and auditing. Cloud providers typically offer basic authentication methods such as user/password and one-time passwords (OTP), which may not adequately secure sensitive resources. Organizations often implement advanced mechanisms like multi-factor authentication (MFA) and public key infrastructure (PKI) authentication, alongside their authorization models, to ensure robust security. Managing multiple authentication options and access control policies across various cloud services can be expensive and complex. Single Sign-On (SSO) systems, which utilize standards like Security Assertion Markup Language (SAML), OpenID Connect, and FIDO2, address this issue by allowing users to access multiple systems with a single set of credentials. These methods enhance security and user convenience but come with costs, compatibility issues, and the risk of single points of failure. Despite the benefits of SSO, relying on cloud-provided authentication services can pose security and privacy risks due to potential identity information leaks. Additionally, managing multiple access policies for various cloud resources is inefficient and costly. To address these challenges, blockchain technology is increasingly adopted for Identity and Access Management (IAM) and data sharing. Blockchain's decentralized, traceable, and tamper-resistant architecture supports scalable and dynamic control of multiple resources, reducing single points of failure. The integration of smart contracts within blockchain frameworks further enhances the enforcement of IAM functions, offering a more secure and efficient solution for managing access control in cloud environments.

II. LITERATURE REVIEW

O. Mir, M. Roland, and R. Mayrhofer. 2022. In current single sign-on authentication schemes on the web, users are required to interact with identity providers securely to set up authentication data during a registration phase and receive a token (credential) for future access to services and applications. This type of interaction can make authentication schemes challenging in terms of security and availability. From a security perspective, a main threat is theft of authentication reference data stored with identity providers. An adversary could easily abuse such data to mount an offline dictionary attack for obtaining the underlying password or biometric. From a privacy perspective,

identity providers are able to track user activity and control sensitive user data. In terms of availability, users rely on trusted third-party servers that need to be available during authentication. We propose a novel decentralized privacy-preserving single sign-on scheme through the Decentralized Anonymous Multi-Factor Authentication (DAMFA), a new authentication scheme where identity providers no longer require sensitive user data and can no longer track individual user activity. Moreover, our protocol eliminates dependence on an always-on identity provider during user authentication, allowing service providers to authenticate users at any time without interacting with the identity provider. Our approach builds on threshold oblivious pseudorandom functions (TOPRF) to improve resistance against offline attacks and uses a distributed transaction ledger to improve availability. We prove the security of DAMFA in the universal composability (UC) model by defining a UC definition (ideal functionality) for DAMFA and formally proving the security of our scheme via ideal-real simulation. Finally, we demonstrate the practicability of our proposed scheme through a prototype implementation.

Y. Berguig, J. Laassiri, and S. Hanaoui, 2021. Recently mobile agent technology used in intelligent systems, cloud computing and IOT. However using mobile agents in distributed environment makes them facing several security threats. In this paper, we propose a lightweight authentication protocol to overcome the security problem, and to provide a secure and anonymous mobile agent system. Our protocol is based on Elliptic Curve Cryptography (ECC) and fulfill all security requirements. For the validation of our security protocol, we used Automated Validation of Internet Security Protocols and Applications (AVISPA) tool using HLPSL language. Furthermore, we used Java Agent Development Framework (JADE) to implement and simulate the proposed scheme. Finally, the paper presents the security analysis and comparison with well-known and significant related protocols in secure communication.

C. Baum, T. Frederiksen, J. Hesse, A. Lehmann, and A. Yanai. 2020. Single Sign-On (SSO) is becoming an increasingly popular authentication method for users that leverages a trusted Identity Provider (IdP) to bootstrap secure authentication tokens from a single user password. It alleviates some of the worst security issues of passwords, as users no longer need to memorize individual passwords for all service providers, and it removes the burden of these service to properly protect huge password databases. However, SSO also introduces a single point of failure. If compromised, the IdP can impersonate all users and learn their master passwords. To remedy this risk while preserving the advantages of SSO, Agrawal et al. (CCS'18) recently proposed a distributed realization termed PASTA (password-authenticated threshold authentication) which splits the role of the IdP across servers. While PASTA is a great step forward and guarantees security as long as not all servers are corrupted, it uses a rather inflexible corruption model: servers cannot be corrupted adaptively and --- even worse --- cannot recover from corruption. The latter is known as proactive security and allows servers to re-share their keys, thereby rendering all previously compromised information useless.

D. Mohan, L. Alwin, P. Neeraja, K. D. Lawrence, and V. Patha. 2022. The Internet of Medical Things (IoMT) is set to create a revolutionary shift in healthcare by transforming traditional methods of disease diagnosis to a data-centered, technology-driven analysis. However, data security and privacy issues are significant hurdles that need to be addressed. Blockchain technology has radically transformed data storage mechanisms using decentralization and cryptographic principles, making it a better choice for sensitive medical data than cloud storage services. A majority of the existing research focus on implementing blockchain in IoT devices which have much higher processing capabilities than IoMT devices such as pacemakers. Most of the existing blockchain frameworks are unsuitable for miniature IoMT devices due to high computational and storage requirements. This work aims to overcome this challenge by proposing a private blockchain framework in which different stakeholders of a medical system such as patients, doctors, IoMT devices, etc. act as nodes, creating a decentralized network in which physiological data output by IoMT devices can be stored securely and tamper free forever. The proposed design is implemented in a Raspberry Pi network, using Proof of Authority (PoA) consensus mechanism which has minimal computational requirements. Data confidentiality is ensured using a double-encryption mechanism by means of Elliptic Curve Integrated Encryption Scheme. It is observed to perform well in comparison with existing approaches with a transaction speed of a minimum of 25 transactions per second and is easily scalable to accommodate different personnel of the healthcare sector. Further development on this design could potentially result in a major innovation in the IoMT industry in the

form of a new array of real-time health monitoring devices with high security and data privacy.

S. Hakak, W. Z. Khan, G. A. Gilkar, B. Assiri, M. Alazab, S. Bhattacharya, and G. T. Reddy. 2020. The rise of blockchain technology within a few years has attracted researchers across the world. The primary reason for worldwide attention is undoubtedly due to its feature of immutability along with the decentralized approach of data protection. As this technology is progressing, lots of developments in terms of identifying new applications, blockchain-based platforms, consensus mechanisms, etc., are taking place. Hence, in this article, an attempt has been made to review the recent advancements in blockchain technology. Furthermore, we have also explored the available blockchain platforms, highlighted and explored future research directions and challenges.

S. K. Kermanshahi, J. K. Liu, R. Steinfeld, and S. Nepal. 2019. If one is to believe the popular press and many “technical writings,” blockchains create not only a perfect transactional environment but also obviate the need for banks, lawyers and courts. The latter will soon be replaced by smart contracts: unbiased and infallible computer programs that form, perform and enforce agreements. Predictions of future revolutions must, however, be distinguished from the harsh reality of the commercial marketplace and the technical limitations of blockchain technologies. The fact that a technological solution is innovative and elegant need not imply that it is commercially useful or legally viable. Apart from attempting a terminological “clean-up” surrounding the term smart contract, this paper presents some technological and legal constraints on their use. It confronts the commonly made claims concerning their ability to automate the transacting process and to ensure perfect performance. It also examines the possibility of reducing contractual relationships into code and the ability to integrate smart contracts with the complexities of the real world. A closer analysis reveals that smart contracts can hardly be regarded as a semi-mythical technology liberating the contracting parties from the shackles of traditional legal and financial institutions. While some of their technical features seem *prima facie* attractive, especially to non-lawyers, a closer analysis reveals their many shortcomings.

III. METHODOLOGY

We assume that the data owner is trusted, and the data users are authorized by the data owner. The communication channels between the owner and users are secure on existing security protocols such as SSL, TLS. With regard to the cloud server, our scheme resists a more challenging security model which is beyond the “semi-honest server” used in other secure semantic searching schemes. In our model, the dishonest cloud server attempts to return wrong/forged search results and learn sensitive information, but would not maliciously delete or tamper with the outsourced documents. Therefore, our secure semantic scheme should guarantee the verifiability, and confidentiality under such a security model.

Existing System Disadvantages

- Organizations without the need for a trusted third party.
- Smart contract enables auto enforcement of the agreed terms between two untrusted parties.

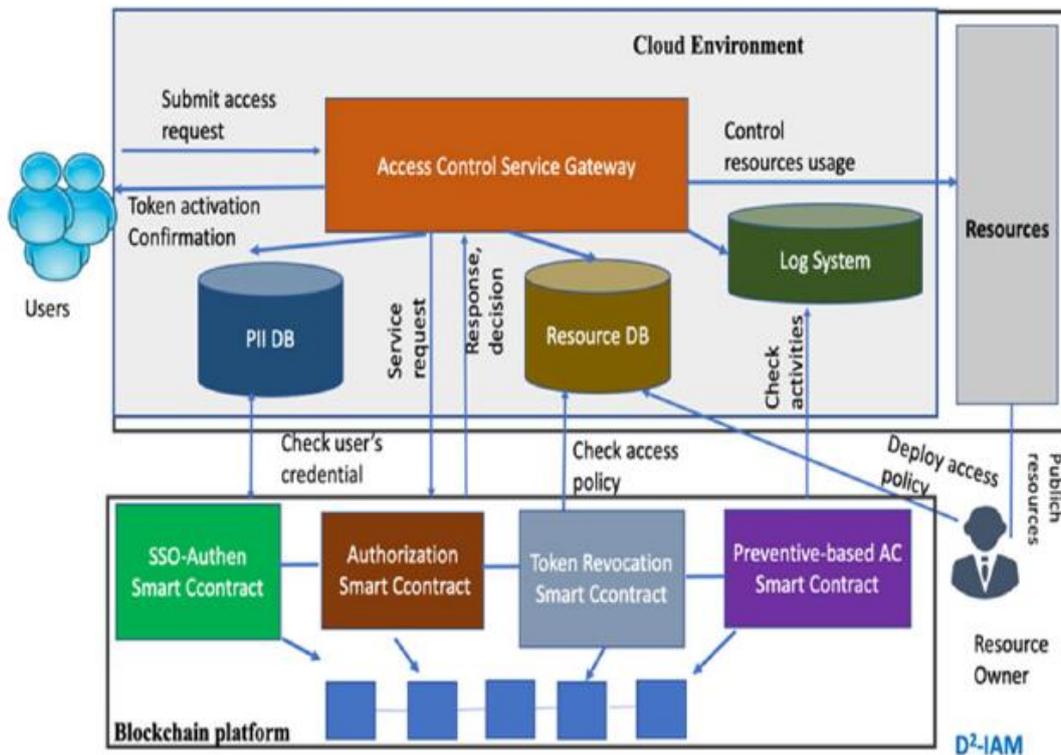
PROPOSED SYSTEM:

We devised a lightweight SSO-authentication token based on highest authentication level of the resources requested to access. The authentication is thus bound to the privilege of resource access instead of relying on additional authentication mechanism. Our proposed SSO-authentication token significantly reduces the communication overhead for multi-system authentication.

Proposed System Advantages

- Smart contract security vulnerabilities, detection tools.
- Ethereum blockchain-based smart contract are highlighted.
- For secure semantic optimal matching on the ciphertext.

SYSTEM ARCHITECTURE



In This Project User has register all details and then login. User can register and upload the document. Next Smart contract can login and create contract. Smart Contract send all files to triggered manager. Next the triggered manager can check users, check files and check registered files. Finally Ethereum block chain will generate hash key and it will store in file.

MODULES:

1. **Client:** In this module we design the windows for the project. These windows are used for secure login for all users. 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 and Email id, into the server. Server 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.
2. **Token:** This is the first module smart contract can register and Login. After login smart contract have an option to create contract. Smart contract can also have a download file it will show an encrypted data. Data user can also send a trapdoor request to the server. Server can accept the the request and then smart contract can takes permissions from the owner then the file it will downloaded in plain text.
3. **Authorization Code:** This is the third module of this project. In this module triggered manager did not have any registration and this module have login only. Triggered Manager will check users, check files and check requested files

also.

- 4. **Block chain Ethereum:** This is the fourth module in this project. This module also have login only and this module will generate hash key and we will see the user files in this module. This is the final module in this project.

IV. IMPLEMENTATION

The project utilizes Java for backend logic, ensuring efficient data processing and business logic implementation. JSP (JavaServer Pages) is employed for dynamic web page generation, seamlessly integrating Java code within HTML for interactive content. This combination of Java and JSP creates a scalable and maintainable web application, ensuring a smooth user experience with responsive features.

V. EXPERIMENTAL RESULTS

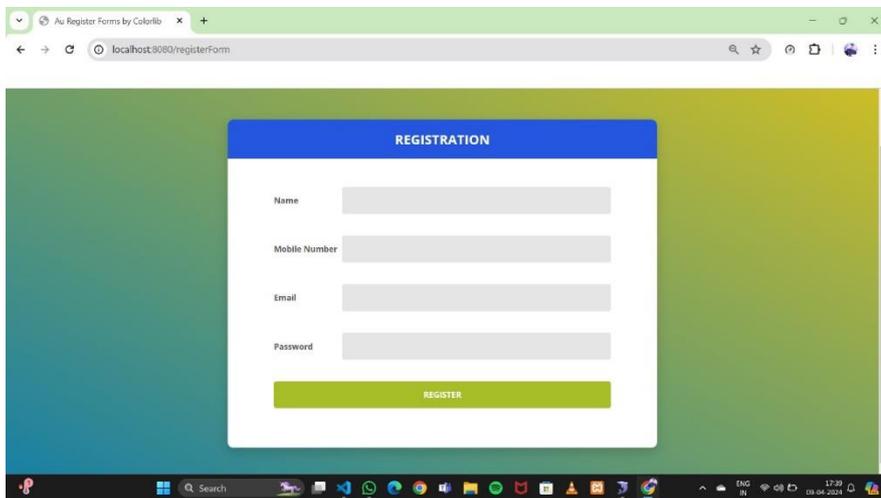
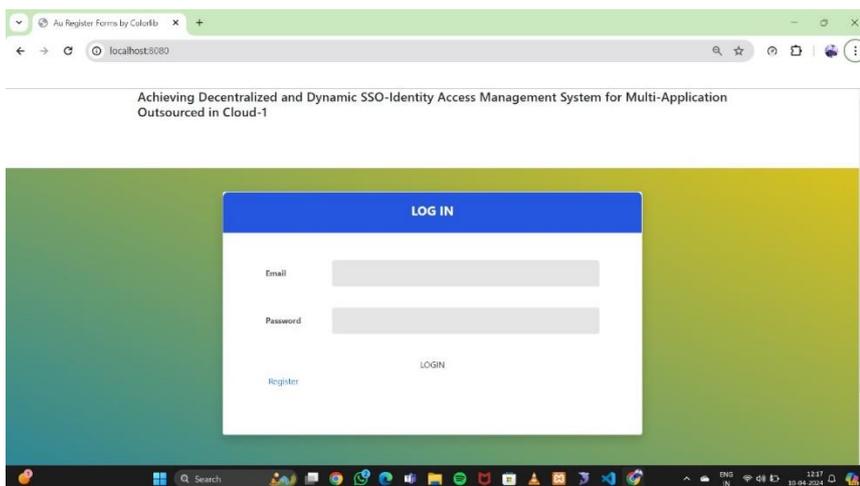


Fig: Data Owner Registration Page



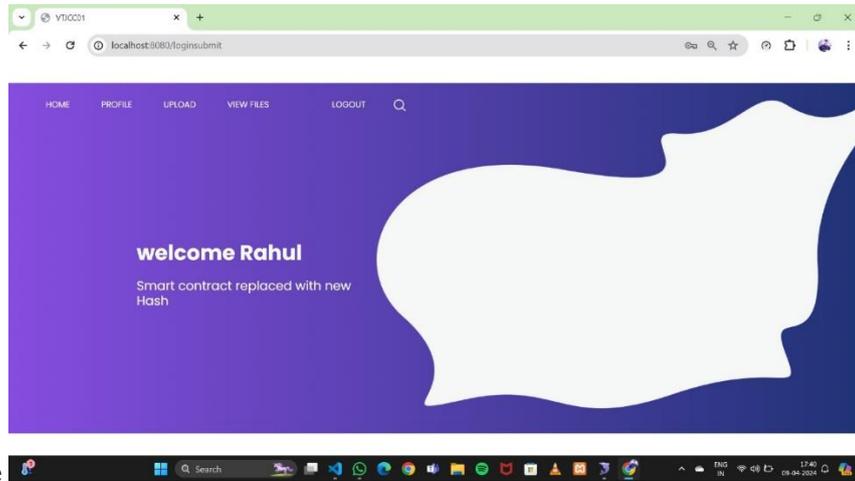


Fig: Data Owner Login Page



Fig: Data Owner Homepage

Fig: Data Owner Upload

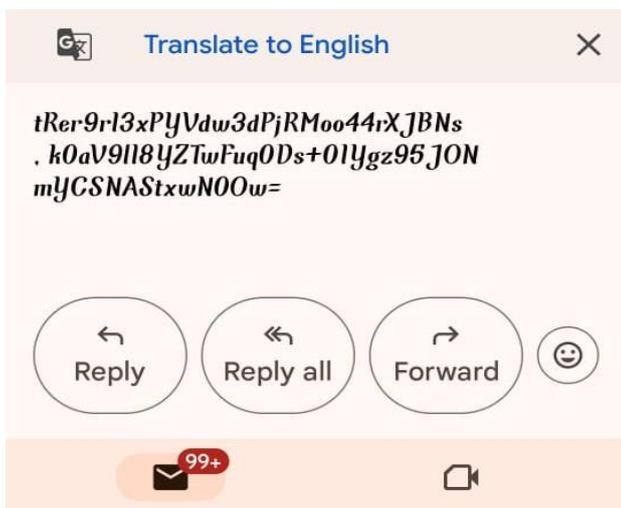


Fig: Data Owner send Keys to User

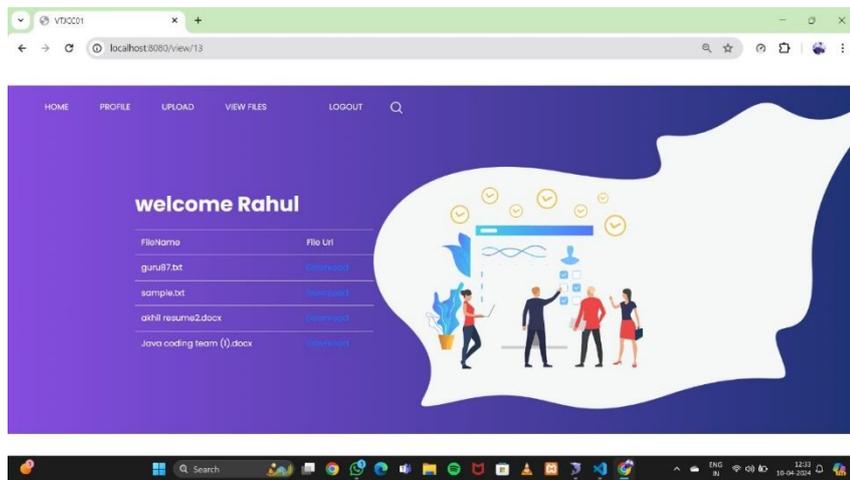


Fig: Data User Download Page

VI. CONCLUSION

We have proposed a blockchain-based access control system called D2 -IAM system to support strong SSO-authentication, dynamic authorization, and preventive-based access control with accountability in cloud computing. Our system optimized the cost of SSO-authentication and authorization process through the design and implementation of smart contracts and blockchains. In addition to achieving high efficiency of authentication and authorization, the access policy is modeled in the document database which is ease of management. Also, the confidentiality of its content is guaranteed based on the public key encryption. We provide the efficiency analysis and experiment to show that D 2 -IAM is efficient in practice and its performance outperforms existing works. For future works, it is a need to devise the auditing protocol to validate the integrity of access policies located on cloud. Even though the policies are encrypted, the assurance of their integrity is still crucial. The public cloud auditing techniques, are worth to explore. In addition, the adoption of decentralized storage platforms, such as Inter Planetary File System (IPFS) for storing the policies, PII database can be used to replace the general cloud storage since IPFS provides more efficient file handling with data indexing.

VII. FUTURE ENHANCEMENT

Developing a machine learning-based anomaly detection method to identify authentication protocol attacks or misuse of Single Sign-On (SSO) authentication tickets is crucial for strengthening digital security. As cloud computing and SSO mechanisms proliferate, the risk of unauthorized access and malicious activities grows. Advanced machine learning techniques offer a proactive defense by analyzing user authentication logs, network traffic, and system events to detect subtle deviations from normal behavior indicative of potential threats. This approach involves data collection, preprocessing, model training, and real-time alerting, leveraging both supervised and unsupervised learning algorithms to distinguish between legitimate and suspicious authentication events. Integrating anomaly detection with real-time alerts allows security teams to swiftly respond to threats, prevent unauthorized access, and enhance authentication controls. Continuous refinement of these models helps adapt to evolving cyber threats, maintaining the integrity and security of authentication protocols in the dynamic digital landscape.

REFERENCES

- [1] S. Fugkeaw, P. Manpanpanich, and S. Juntapremjitt, "Exploiting X.509 certificate and multi-agent system architecture for role-based access control and authentication management," in Proc. 7th IEEE Int. Conf. Comput. Inf. Technol. (CIT), Oct. 2007, pp. 733–738.
- [2] The Open ID Connect. Accessed: Jan. 14, 2023. [Online]. Available: <https://openid.net/connect/>
- [3] F. F. Moghaddam, P. Wieder, and R. Yahyapour, "A policy-based identity management schema for managing accesses in clouds," in Proc. 8th Int. Conf. Netw. Future (NOF), Nov. 2017, pp. 91–98.
- [4] N. Naik and P. Jenkins, "A secure mobile cloud identity: Criteria for effective identity and access management standards," in Proc. 4th IEEE Int. Conf. Mobile Cloud Comput., Services, Eng. (MobileCloud), Mar. 2016, pp. 89–90.
- [5] S. Wang, R. Pei, and Y. Zhang, "EIDM: A Ethereum-based cloud user identity management protocol," IEEE Access, vol. 7, pp. 115281–115291, 2019.
- [6] N. Hossain, M. A. Hossain, M. Z. Hossain, M. H. I. Sohag, and S. Rahman, "OAuth-SSO: A framework to secure the OAuth-based SSO service for packaged web applications," in Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng., New York, NY, USA, Aug. 2018, pp. 1575–1578, doi: 10.1109/TRUSTCOM/BIGDATAASE.2018.00227
- [7] C. Tang, X. Fu, and P. Tang, "Policy-based network access and behavior control management," in Proc. IEEE 20th Int. Conf. Commun. Technol. (ICCT), Oct. 2020, pp. 1102–1106.
- [8] H. Zhou and L. Zhu, "Research and design of CAS protocol identity authentication," in Proc. Int. Conf. Comput. Vis., Image Deep Learn. (CVIDL), Jul. 2020, pp. 384–387.
- [9] M. A. Thakur and R. Gaikwad, "User identity and access management trends in IT infrastructure—An overview," in Proc. Int. Conf. Pervasive Comput. (ICPC), Jan. 2015, pp. 1–4.
- [10] M. Uddin, S. Islam, and A. Al-Nemrat, "A dynamic access control model using authorising workflow and task-role-based access control," IEEE Access, vol. 7, pp. 166676–166689, 2019.