Decentralized Identity and Access Management of Cloud for Security as a Service

Soumya Prakash Otta
Research Scholar, Dept of CSIS
BITS PILANI,
Hyderabad, India
p2016300@hyderabad.bits-pilani.ac.in

Dr Subhrakanta Panda
Assistant Professor, Dept of CSIS
BITS PILANI
Hyderabad, India
spanda@hyderabad.bits-pilani.ac.in

2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS) | 978-1-6654-2104-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/COMSNETS53615.2022.9668529

***Abstract*—Many cyber-related untoward incidents and multiple instances of a data breach of system are being reported. User identity and its usage for valid entry to system depend upon successful authentication. Researchers have explored many threats and vulnerabilities in a centralized system. It has initiated concept of a decentralized way to overcome them. In this work, we have explored application of Self-Sovereign Identity and Verifiable Credentials using decentralized identifiers over cloud.**

***Index Terms*—Decentralized Identity, DID, Distributed Ledger, Identity-Access Management**

I. Introduction

From standalone to complex networked systems, the end-user is the crucial entity for effective utilization and reap rich dividends of technology. Users of such systems are identified by either physical or digital, or cryptographic credentials. From this point of view, user Identity and access management (IAM) security is regarded as an essential and integral constituent of IT security system [1].

The concept of virtuality and unlimited amount of IT resources provisioning has given rise to on-demand and metered provisioning of IT resources with 'As a Service' approach. With increasing number of tenants for a Cloud infrastructure-based ecosystem, management has a significant challenge for Cloud Service Providers (CSP). Hence, the CSPs require an efficient IAM.

WWW has been overriding on data centers of various CSPs. World Wide Web Consortium (W3C) has come up with several modern and efficient means for secured information exchange over WWW. The W3C promotes decentralized Identifiers (DIDs) to address IAM-related challenges. Using DID, nuances of centralized IAM-related challenges can be easily addressed by implementing a decentralized IAM solution. In this approach, desired databases are implementable with DID compatible Blockchain. Distributed Ledgers (DL) are DID Compatible. This fundamental infrastructure of the decentralized identity-based solution is the critical factor in establishing a trust relationship between verifiable credentials (VC) and DID provisioned user entities [2] of the system.

This paper presents a decentralized IAM framework incorporating DIDs and VCs and smart contracts over Ethereum Blockchain. A detailed analysis has been covered along with its insights of implementation.

II. Blockchain Based Identity and Access Management

The most of DL based system have been implemented with Blockchain technology. The second generation of Blockchain has been successfully implemented in platforms like Ethereum and is currently under development leading to Ethereum 2.0 in the third generation. Ethereum has been successfully implemented in ecosystems like Hyperledger.

Everything as a service model of Cloud Computing (CC) has posed several challenges due to associated vulnerabilities [3]. Hence, the concept of Security as a Service plays a vital role in adopting and taking advantage of CC systems. Among the deciding factors of providing Security as Service, user identity, and its authorization for cloud resources are considered the most vital factors. Relevant aspects of Cloud IAM are as follows.

A. Authentication Management

Identity management of a system has a defined standard to create, maintain, and de-provision user accounts. Stable and robust identity management and its procedural enforcements are required for managing and maintaining user identities. The first objective is to facilitate new users' trouble-free and secure way to access system resources and services. Second, timely de-provisioning of users ensures legitimate users have access to services and system resources. Authentication checks something the user already know (like a password) or something the user has (like a hardware dongle),something the user is having (like user biometric) or even where the user is (like location). Legacy system had centralized and Independent Identity Management [4] where user were required to have a separate identity and its credential for each system to access multiple systems.

A new concept called Self-sovereign identity (SSI) is emerging [5], where users can control their own digital identity. The mechanism is independent of any TTP for identity management. In this, users can store their identity related credentials and other information on their owned devices which are permitted to be produced for identity validation. Main characteristics of this identity authorization method are user portability, user security, and total control over own credentials. From the user browser and W3C point of view,

the Open ID Connect standard is capable of performing the verifier role in SSI terminology.

Authentication using Blockchain use immutable property of DL. The DL is used to verify ledger entries to check and verify genuineness of users, their transactions, and associated message transfer as events. These events are stored in blocks in read-only manner for future reference and verification. Blockchain authentication [6] mechanism operates with deployed smart contracts over the Blockchain. Inspired by this, in the presently proposed Smart Contract Engine for IAM (SCE-IAM) activation for every authentication request by either user identity provider, verifier, or CSP, a pre-defined set of actions can be triggered. Using this, dependency on a TTP is eliminated.

B. Authorization Management

Access control is an essential mechanism for Authorization Management to prevent unauthorized access to secured resources. Another aim of this is to maintain user privacy and data security. Traditionally, access control methods adopted in a Cloud scenario are based on well-established access control policies of CSP. Well-established access control policies are categorized considering four specific aspects like Discretionary Access Control (DAC) [7], Mandatory Access Control (MAC), Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC) [8]. A systematic comparison of the inherent advantages and disadvantages given in [9] gives an overall approach to the concept and mitigation of drawbacks.

Apart from being vulnerable to a single point of failure, centralized authentication system have definite limitations on transparency, traceability, resistance to tampering, and simultaneous control by multiple stakeholders [10].

III. BLOCKCHAIN BASED CLOUD IAM

DL technology and Blockchain's benefits are considered effective against legacy access control methods [11]. Blockchain-Based Access Control (BBAC) can have two specific advantages. Firstly, BBAC can enforce a consensus mechanism for access control to have simulations control by multiple stakeholders. It could enhance cloud security by decentralization. Secondly, governance and controlling capability for access control could be made effective using time stamping and immutable nature of Blockchain entries.

Several research works have contributed many aspects of modern applications and advantages for Security as a Service (SECaaS) for Cloud based system applications [12].

Using a Blockchain-based system with a smart contract for Security of Virtual Machine (VM) and control over their access to the systems physical machines was considered in [13]. Such access control helped in preventing threats arising from side-channel analysis and attacks on system. Novo et al. [14] proposed a singular smart contract-based system for managing the system access policies. Concept of management hub was introduced to manage many edge devices which are allowed access to the blockchain network.

A blockchain framework for attribute-based fine-grained access control has been proposed using distributed storage system by Wang et al. [15]. The conventional attribute-based encryption was primarily dependent on the trusted Public Key Generator (PKG) mechanism. In this work, Blockchain was additionally responsible for key management rather than only handling trusted PKG related tasks. In BlockSLaaS [16], a blockchain-enabled mechanism was proposed to provide Logging-as-a-Service (LaaS). Apart from access control techniques, this mechanism handles cloud forensics using Blockchain.

For avoidance of single-point failure, possible misutilization of secured and sensitive data by TTP, a blockchain has been applied [17] in a decentralized access control mechanism. As an effective access control mechanism, owners have complete control over access of their owned data with blockchain technology. A Blockchain-based access control work proposed by Wang et al. [18] is capable to avoid possible ill effects caused by unreliable third parties or users having doubtful honesty using decentralization method. Nguyen et al. [19] examined the performance of Blockchain-based access control using medical records for trustworthiness in access controls.

Lin et al. [20] have analyzed and compared various features of Blockchain-based IAM solutions with a comprehensive analysis of their features and corresponding advantages offered. In [21] Liu et al. have brought out a detailed comparative analysis of Blockchain-based IAM solutions specifically considering authentication, privacy and trust.

IV. PROPOSED SYSTEM FRAMEWORK

This paper proposes a novel framework towards attaining SECaaS by Secured and Decentralized IAM based on above discussion and various work done in DL-based applications. This approach incorporates the advantages of DL-based system and work for mitigation of disadvantages of centralized IAM systems.

A. System Overview

W3C compatible standards for authentication are Open ID Connect on the OAuth 2.0 framework. Using this benchmark, we have designed and propose a new novel IAM framework using DL technique coupled with DID for a cloud. In this proposed system, cloud user identity maps to DID. Using smart contracts over an Ethereum based Blockchain that aims to interact with the DL of Blockchain, provides desired authentication and authorization for cloud resources. User identity and their credential storage uses Inter Planetary File System (IPFS).

Different ten number of architectures for DID-based authentication has been described in DID Auth document written by Sabadello et al [22]. Such integration is covered in WebAuthn [23]. The Javascript Object Signing and Encryption (JOSE) method documentation is compatible for decentralized authentication with a self-assigned ID token using Open ID Connect standard. However, JOSE must access a Universal Resolver

instance for getting desired keys for DID authentication. Considering this, we propose a Smart Contract Engine for Identity and Access Management (SCE-IAM) Model using the self-assigned ID token for users. This makes use of two mutually integrated Smart Contracts deployed over a Blockchain. The Smart contract's integration and intercommunication mechanism are handled with RFC 7519 based Java JSON Web Token (JWT).

B. System Architecture

From a cloud user authentication and authorization point of view, four definite steps are considered while using cryptographic credentials. Firstly, the registration of cloud user identity and credentials. Secondly, identity credential-related information retrieval and verification. Thirdly, smart contract development and deployment. Fourthly, cloud resource access control and management via smart contract. The overall system architecture is presented in Figure 1. The proposed system has various well-defined and specific modules to address desired set of activities.

Further, the IAM actions are involved in transforming identity as triggered by Smart Contract, identity access control, and finally, the process of identity verification. The identity transformation involves hashing algorithms utilization for secured transformation and storage retrieval. The activation condition of the smart contract enforces the identity access control policies. Finally, the identity verification is performed as mentioned in the SSI verification process using a standard three-way verification mechanism.

C. System Workflow

Main players in overall system are the cloud user, the CSP or identity provider, the DID Client, the user's Digital Wallet, and the Distributed Ledger. Knowledge of DIDs about users is a prerequisite for the SSI-enabled Open ID Connection Provider. Accordingly, the proof request could only be sent to the respective user. An interactive flow diagram among the stakeholders is shown in Figure 2.

D. Modules And Function

The following crucial modules are covered as system design descriptions. A homogenous interactive interrelationship among the below-mentioned modules is essential for implementation.

User registration The User IAM process gets initiated with user registration. For enabling interactions between cloud users and the Blockchain, a crypto-wallet is required. The wallet contains the corresponding user's private/public key pair and the corresponding blockchain address. Registered user's credentials thus collected are stored in the IPFS system having its return hash ID. Subsequently, hash ID and the user ID are transformed into a new hash value using hash function.

Generation and Operation of VC Register a DID for a user on the Blockchain through a Smart contract requires a VC from the CSP. CSP generates a VC after user registration is done and the hash ID of the user is created. This VC is responsible for the verification of presented credential for user authentication. Significantly, user authentication is handled by Smart contract deployed over Ethereum.

DID Registration We have assumed that the DID subject for W3C access is the DID holding user for this work. As far as user credentials registered with CSP are concerned, the user is described as the DID owner. The DID controller is responsible for the authentication process, which is further required for authorization to get the same accessed through the user browser.

Data Auth by DID The DID methods in use and the related bounded applications check and establish authorization status for DID Controllers. Such authorization check is performed after the completion of authentication process. It is termed DID Auth. [24] DID Auth works in three-step process. Firstly, the DID's registered user or owner transfers a DID with a verification request for its authentication. Secondly, the DID resolver performs the verification to obtain the desired DID Document matching with the verifiable data registry. In the third and final step, the verifier encrypts the DID Document that matches the DID of Controller by using a random temporary value as the public key. The random temporary public key is called the nonce in terms of Blockchain. Ultimately, DID owner (genuine user) decrypts the challenge by using their private key.

Smart Contract Activity The proposed SCE-IAM uses two different Smart contracts deployed over the Ethereum Blockchain. The first one is dedicated to handling the user identity authentication-related activities. In comparison, the second one is responsible for user authentication for the cloud resources. Both function seamlessly with the implementation of JWT based integration and sharing the standard DL from the Ethereum Blockchain.

V. IMPLEMENTATION AND ANALYTIC EVALUATION

A test setup was created to implement the proposed DID-enabled Blockchain-based decentralized IAM using the SCE-IAM mechanism.

A. Execution

AWS cloud infrastructure with eight Virtual Server Machines running Ubuntu 18.04 with 16 GB resident memory and 500 GB storage was used. Thirty cloud users were created for testing purposes. For Blockchain realization Hyperledger Indy was chosen and configured over the AWS cloud setup. For implementing SSI-based and Open ID Connect (OIDC) integration, we have used Hypervisor Indy Edge Agent API. For functionality of the Hyperledger Indy SDK, an agent REST API deployable on a server is used. The clients are provisioned with REST calls for SDK functionality. The SSI functionality towards the signing of token and their verification jwt.io of the JOSE library was used. React Native Android app development method was used for authentication app for OTP/PIN authentication for DID integration of hashed user IDs. Python 3.6.4 programming was used for simulating users,

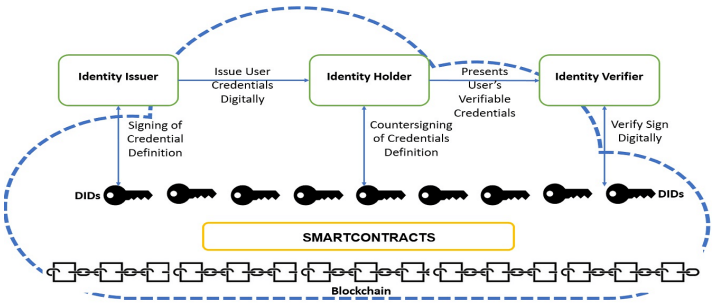

Fig. 1. System Architecture of DID enabled Blockchain Powered Cloud IAM

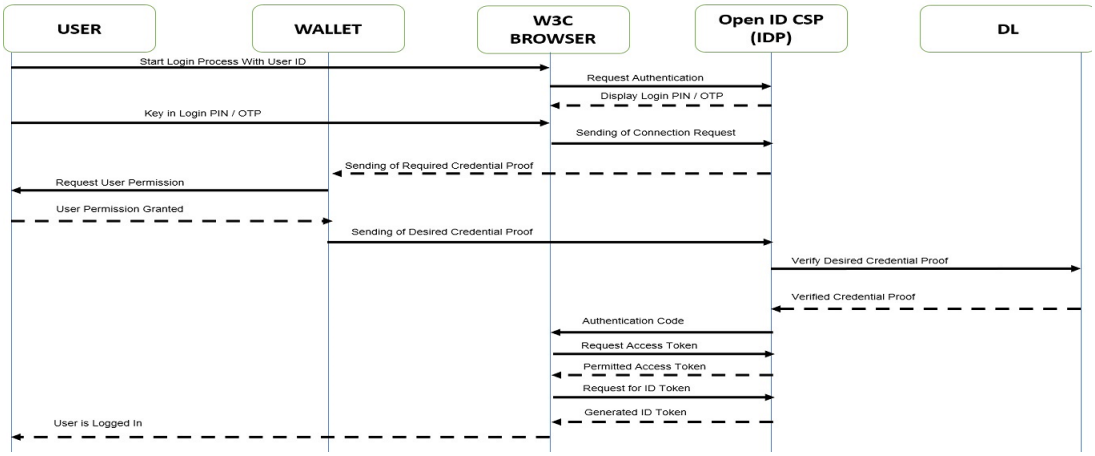

Fig. 2. Workflow Model of Proposed Approach

having authorities and also verifiers. It also facilitates linking with IPFS to access data of user using a hash ID. Solidity (0.4.24) language was used for programming of the Smart Contracts.

B. Evaluation

An IAM exercise for registration, authorization and verification was conducted for checking the time taken for the above setup. The results obtained from the setup were found to be promising. Table I summarizes the results obtained for the Thirty users set up using the AWS Cloud for Decentralized IAM set up with DID-enabled user access for designated Cloud resources. As DIDs mainly affect performance of the front-end aspects using a W3C compatible browsers, we have assumed the time factor as negligible and not critically relevant for this performance evaluation.

C. Threat modeling and analysis

A potential breach that could compromise the user's private key may prove disastrous since user's private key's safety is found to be the weakest link. Since DID is generated randomly, the ownership of this lies with the user. Hence a malicious user threat could not be ruled out. A recent research [25] by Rhie et al. has brought out some more and exciting challenges towards DID updation for Decentralized identifiers.

TABLE I
PERFORMANCE EVALUATION OF PROOF OF WORK

SER No	STAGE	ACTIVITY	TIME (In Sec)
1	User Registration	Mapping of User IDs from CSP IDP to Blockchain	4
2	User Registration	User ID hashing and storing to IPFS	2
3	User Registration	Constructing the Smart Contract	9
4	Authorization	Adding addresses to Smart Contract	10
5	Identity Verification	Retrieval of Hash	10
6	Identity Verification	Verification of Hash	1
7	Identity Verification	Retrieval from IPFS	2
8	Identity Verification	PIN/OTP Comparison function	1

VI. CONCLUSION

SECaaS for Cloud-based system is achievable to make the security aspects provisioned for Cloud. Among the factors, IAM has been analyzed in this work to make it possible with a decentralized approach. This work has also incorporated the state-of-the-art security mechanism in DID and Blockchain for secured web access for the Cloud authenticated users. Its inbuilt time stamping feature is suitably applied for system administration and control. Further, such properties are open to being explored towards time-stamped event logging and Cloud forensic applications. However known weakness and vulnerabilities of Ethereum based systems needs specific attention.

REFERENCES

[1] Tabrizchi, Hamed, en Marjan Kuchaki Rafsanjani. "A survey on security challenges in cloud computing: issues, threats, and solutions". *The journal of supercomputing* 76, no 12 (2020): 9493–9532.

[2] Manu Sporny, Dave Longley, and David Chadwick. 2019. Verifiable Credentials Data Model 1.0 - Expressing verifiable information on the Web. [Online]. Available: https://www.w3.org/TR/vc-data-model/(Accessed August 15, 2021).

[3] Subramanian, Nalini, en Andrews Jeyaraj. "Recent security challenges in cloud computing". *Computers and Electrical Engineering* 71 (2018): 28–42.

[4] Khajehei, Kamyab. "Role of identity management systems in cloud computing privacy". *International Journal of Education and Management Engineering* 7, no 3 (2017): 25–34.

[5] Mühle, Alexander, Andreas Grüner, Tatiana Gayvoronskaya, en Christoph Meinel. "A survey on essential components of a self-sovereign identity". *Computer Science Review* 30 (2018): 80–86.

[6] Lim, Shu Yun, Pascal Tankam Fotsing, Abdullah Almasri, Omar Musa, Miss Laiha Mat Kiah, Tan Fong Ang, en Reza Ismail. "Blockchain technology the identity management and authentication service disruptor: a survey". *International Journal on Advanced Science, Engineering and Information Technology* 8, no 4–2 (2018): 1735–45.

[7] Lopez, Javier, en Juan E. Rubio. "Access control for cyber-physical systems interconnected to the cloud". *Computer Networks* 134 (2018): 46–54.

[8] Qiu, Meikang, Keke Gai, Bhavani Thuraisingham, Lixin Tao, en Hui Zhao. "Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry". *Future Generation Computer Systems* 80 (2018): 421–29.

[9] Tabrizchi, H. and Rafsanjani, M.K., "A survey on security challenges in cloud computing: issues, threats, and solutions". *The journal of supercomputing* 76, no 12 (2020): 9493–9532.

[10] Salman, Tara, Maede Zolanvari, Aiman Erbad, Raj Jain, en Mohammed Samaka. "Security services using blockchains: A state of the art survey". *IEEE Communications Surveys and Tutorials* 21, no 1 (2018): 858–80.

[11] Min, Hokey. "Blockchain technology for enhancing supply chain resilience". *Business Horizons* 62, no 1 (2019): 35–45.

[12] Hawedi, Mohamed, Chamseddine Talhi, en Hanifa Boucheneb. "Security as a service for public cloud tenants (SaaS)". *Procedia computer science* 130 (2018): 1025–30.

[13] Zhang, Yuanyu, Shoji Kasahara, Yulong Shen, Xiaohong Jiang, en Jianxiong Wan. "Smart contract-based access control for the internet of things". *IEEE Internet of Things Journal* 6, no 2 (2018): 1594–1605.

[14] Novo, Oscar. "Blockchain meets IoT: An architecture for scalable access management in IoT". *IEEE Internet of Things Journal* 5, no 2 (2018): 1184–95.

[15] Wang, Shangping, Yinglong Zhang, en Yaling Zhang. "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems". *IEEE Access* 6 (2018): 38437–50.

[16] Rane, Sagar, en Arati Dixit. "BlockSLaaS: Blockchain assisted secure logging-as-a-service for cloud forensics". *In International Conference on Security and Privacy*, 77–88. Springer, 2019.

[17] Rouhani, Sara, en Ralph Deters. "Blockchain based access control systems: State of the art and challenges". *In IEEE/WIC/ACM International Conference on Web Intelligence*, 423–28, 2019.

[18] Wang, Shangping, Xu Wang, en Yaling Zhang. "A secure cloud storage framework with access control based on blockchain". *IEEE Access* 7 (2019): 112713–25.

[19] Nguyen, Dinh C., Pubudu N. Pathirana, Ming Ding, en Aruna Seneviratne. "Blockchain for secure ehrs sharing of mobile cloud based e-health systems". *IEEE access* 7 (2019): 66792–806.

[20] Lim, S.Y., Fotsing, P.T., Almasri, A., Musa, O., Kiah, M.L.M., Ang, T.F. and Ismail, R., "Blockchain technology the identity management and authentication service disruptor: a survey". *International Journal on Advanced Science, Engineering and Information Technology* 8, no 4–2 (2018): 1735–45.

[21] Liu, Yang, Debiao He, Mohammad S. Obaidat, Neeraj Kumar, Muhammad Khurram Khan, en Kim-Kwang Raymond Choo. "Blockchain-based identity management systems: A review". *Journal of network and computer applications* 166 (2020): 102731.

[22] M. Sabadello, K. Den Hartog, C. Lundkvist, C. Franz, A. Elias, A. Hughes, J. Jordan, and D. Zagidulin. (2018) Introduction to DID Auth. Rebooting the Web of Trust. [Online]. Available: https://github.com/WebOfTrustInfo/rwot6-santabarbara/blob/master/final-documents/did-auth.md

[23] C. Brand, A. Langley, G. Mandyam, M. West, and J. Yasskin, (2019), "Web Authentication: An API for accessing Public Key Credentials Level 1," [Online]. Available: https://www.w3.org/TR/webauthn/ .(Accessed Septmber 15, 2021).

[24] Markus Sabadello et al., "Authentication's White Papers: Introduction to DID Auth," Rebooting the Web of Trust, 31 July 2018. [online] Available: https://www.weboftrust.info/papers.html(Accessed October 22, 2021).

[25] Rhie, Min-Hyung, Kyung-Hoon Kim, Dongyeop Hwang, en Ki-Hyung Kim. "Vulnerability Analysis of DID Document's Updating Process in the Decentralized Identifier Systems". *In 2021 International Conference on Information Networking (ICOIN)*, 517–20. IEEE, 2021.