IDENTITY AND ACCESS MANAGEMENT FOR FINANCIAL INDUSTRY

Kalaivani B

kala20204.cs@rmkec.ac.in

R.M.K. Engineering College

Padma Priya V

padm20239.cs@rmkec.ac.in

R.M.K. Engineering College

Abstract

Identity and Access Management (IAM) systems are crucial for any information system, especially financial institutions. Financial organizations that hold consumer data, in particular those that provide financial services to retail and commercial customers, including banks, investment companies, real estate firms, retail banking and insurance companies, are an obvious target for the simple fact that this is where the money is. If there is a vulnerability, it will be the first target. In response, banks and financial institutions require tailored and sophisticated security to support their systems and people, and to defend against an onslaught of complex and aggressive cyber-attacks. This proposed system aims at secured transactions and access management implemented using the Block-chain concept. Block-chain technology comes in handy for IAM solutions that not only require a comprehensive security framework but also scalability at the same time. Having a secure framework is made possible by performing a background analysis on the users' profile. Knowing the users will make it easier to segregate the roles. Identification of user roles will allow the owner of the organization to easily monitor who is accessing what and also track the occurrence of any unusual activity.

Keywords: Identity and Access Management (IAM), Block-chain, Financial Institutions, Vulnerability, Security

I. INTRODUCTION

In today's scenario, people are into digitizing every application considering the ease of usage. When it comes to money related subjects, there is a huge demand for reliability and certainty among transactions. Between strict data regulations and evolving cyber threats, the financial industry has no room for error when it comes to securing customer and company data. Data security is considered to be the most important aspect in terms of financial transactions. It remains a constant challenge for the consumer-centric financial industries to secure and manage identities while providing convenient, seamless, and real-time access that the customers may demand.

The Banking and Financial Institutes (BFIs) often face an increasing number of threats from targeted attacks to Distributed Denial-of-Service (DDoS), and from phishing to point-of-sale and ATM security issues. At this juncture, Identity and Access Management (IAM) has emerged as the need of the hour. IAM is the secure choice for financial institutions to provide authorized access to information at any time, from anywhere, for employees and businesses. The IAM solutions are hence contributed by Block-chain technologies.

Block-chain technology produces a structure of data with inherent security qualities. It is based on principles of cryptography, decentralization and consensus, which ensures trust in transactions. In most block-chains or Distributed Ledger Technologies (DLT), the data is structured into blocks and each block contains a single transaction or bundle of transactions. This paper confers the following contributions:

- To set up a commercial User Life-cycle management for performing Create, Review, Update, Deactivate (CRUD) operations securely.
- To improve authentication and encrypt data using Secure Shell.
- To establish Segregation of Duties (SoD) that enforces operational checks and balances.
- To apply Private Block-chain mechanism for improving access control and performance in accounting firms.

II. LITERATURE SURVEY

[1] The article presents an extensive literature review of commercial market offerings regarding the applicability of BC-based Self Sovereign Identity (SSI) solutions. It also provides details regarding the building blocks of block-chain technology and a progressive road-map of International Data Management Systems (IDMS) solutions. In order to develop an effective BC-based IDMS solution that focuses on securing a user's SSI, this article outlines five essential components.

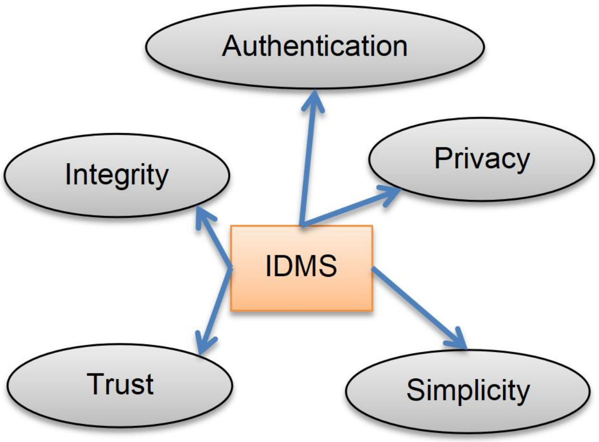


Fig.1. Components of BC-based IDMS Solutions

Furthermore, a security analysis that outlines several types of adversarial threats that can cause potential damage to the BC-based IDMS is performed.

Identifying one's identity seems to be the prime approach towards preventing unwanted attacks either from the insider or from the external shareholders.

[2] Block-chain has many other potential financial applications like mainstream payment, securities issuance, clearing and settlement, derivatives and other financial instruments, trade repositories, credit bureaus, corporate governance, etc. Open source software implementations that run on Linux operating systems have been actively developed and maintained. To combine protocols with user interfaces and to formalize secure relationships over computer networks, smart contracts are also proposed as a solution in public environments depending on a trusted third party to accomplish the automation.

[3] The importance of Identity and Access Management (IAM) when dealing with main business processes is being stressed out. Being able to detect unusual access and outlier forms is absolutely necessary for a manager to be able to address many of the challenges in each of the IAM's major areas. Identity management implies data analysis, reporting and ongoing monitoring, modeling and efficient decision making processes. The problem itself is very complicated because the lack of access leads to direct losses of productivity along with other indirect losses.

[4] The issues related to authentication, access management, security and services in the cloud environment are surveyed along with the techniques proposed to overcome the same. The major contributions of the paper are: Comparative and overview analysis of different aspects in identity and access management mechanisms in the cloud environment. Overview of common security threats in Cloud IAM systems and prevention techniques.Recommendations on governance policies and industry best practices.

[5] This paper examines the use of block-chains implemented in accordance with financial investments. An overview of the concept of block-chain technology and its potential to change the world of banking through facilitating global money remittance, smart contracts, automated banking ledgers and digital assets has been provided. This study presents issues and countermeasures related to Korea's related fields through the case of application of block-chain based finance in foreign countries.

III. METHODOLOGY

1) CRUD Mechanism:

CRUD is an acronym that's famous in the world of computers and refers to the four functions that are mandatory for constructing an efficient storage application.

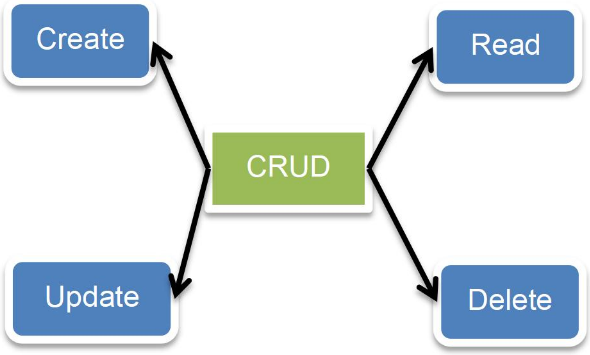


Fig.2. The acronym CRUD

Starting with creation of a self-service module with password reset abilities will provide immediate commercial advantage. Creating a single sign-in is a prime method of authentication where no one can pretend to be anyone else. Biometric, two factor authentication, or even better multi factor authentication methods are implemented to know the users who are connected in the network. This step allows each user to know every other user who is being part of the organization.

To improve authentication and provide scalability and feasibility to the service providers, an industry standard protocol OAuth 2.0 comes into the picture. OAuth 2.0 defines four roles:
i. Resource Owner (end-user), which is an entity that has the ability to provide access to a restricted resource.
ii. The resource server and the protected resources are hosted on this server.
iii. Client application generally operating on a mobile device or a conventional web application requests access to a protected resource.
iv. The authorization server, which follows the OAuth 2.0 protocol, checks the user's identity before issuing access tokens to the application.

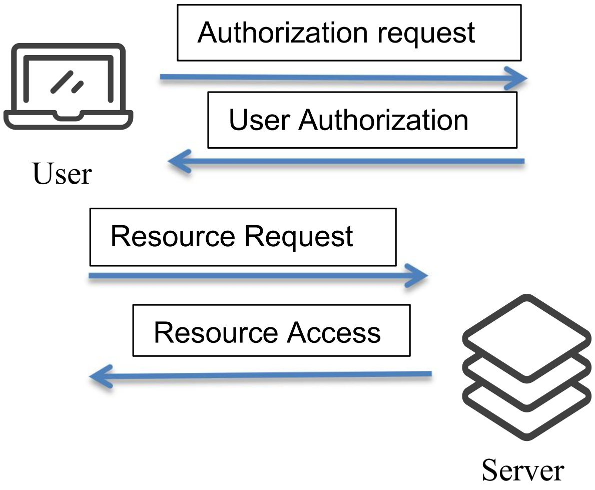
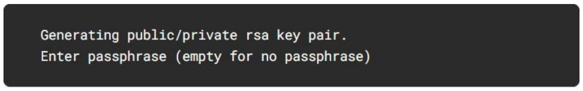


Fig. 3. Steps in OAuth 2.0 protocol

2) SSH:

SSH is a cryptographic network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network. It is ubiquitous within the financial services industry. SSH provides strong authentication and encrypted data communications between two computers in the banking or other financial orientation connecting over an open network such as the internet. Banks, insurance companies, brokerages, credit unions, etc. all use Secure Shell for business processes critical to day-to-day operations and for bringing new services online.

SSH key agents store the private keys and provide them to the SSH client programs. These private keys are encrypted with passphrases that are provided during each attempt to connect with the server. In every individual invocation of SSH, the passphrases are needed to decrypt the private key before proceeding to the authentication phase.



```
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase)
```

Fig. 4. SSH in Google Cloud service provider

The main advantage of SSH keys is that the authentication to the server is performed without passing the password over the network. This prevents the interception or cracking of the password by hackers. The attempts of guessing credentials through brute force attacks during authentication are eliminated by SSH keys.

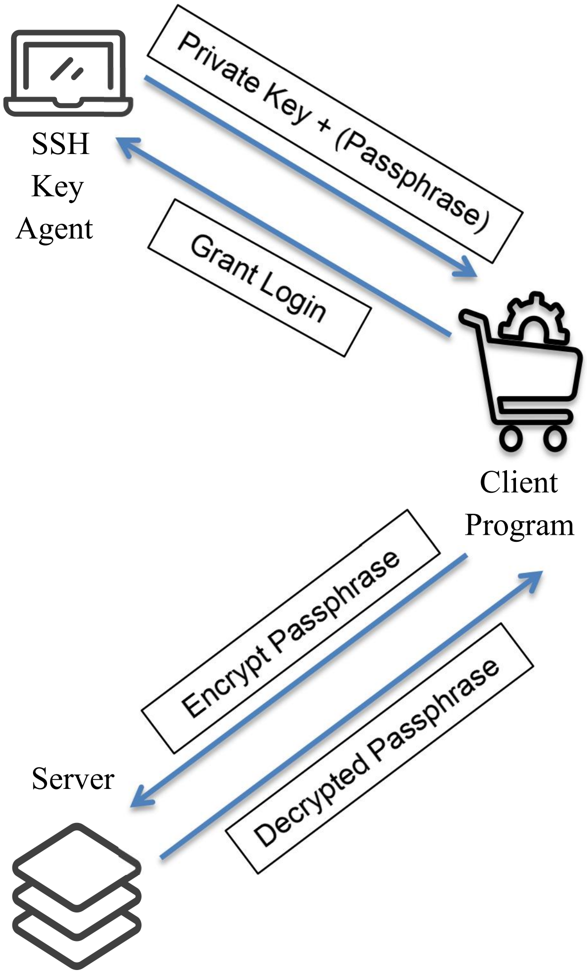


Fig.4. Secure Shell

Poor controls over Secure Shell environments have contributed to costly data breaches and compliance violations. Static credentials and SSH key mechanisms are commonly used for cloud web service authentication.

3) SoD:

Segregation of Duties is implementing a process for role management, that is designing an access management framework for both internal and external users. SoD is mandatory because it strengthens the trust of an industry by sorting out which user will have access to which facility and also identifies a new user who is trying to access the data. Hence, to promote good decision making and pitching of an organization, SoD is considered to be an important procedure.

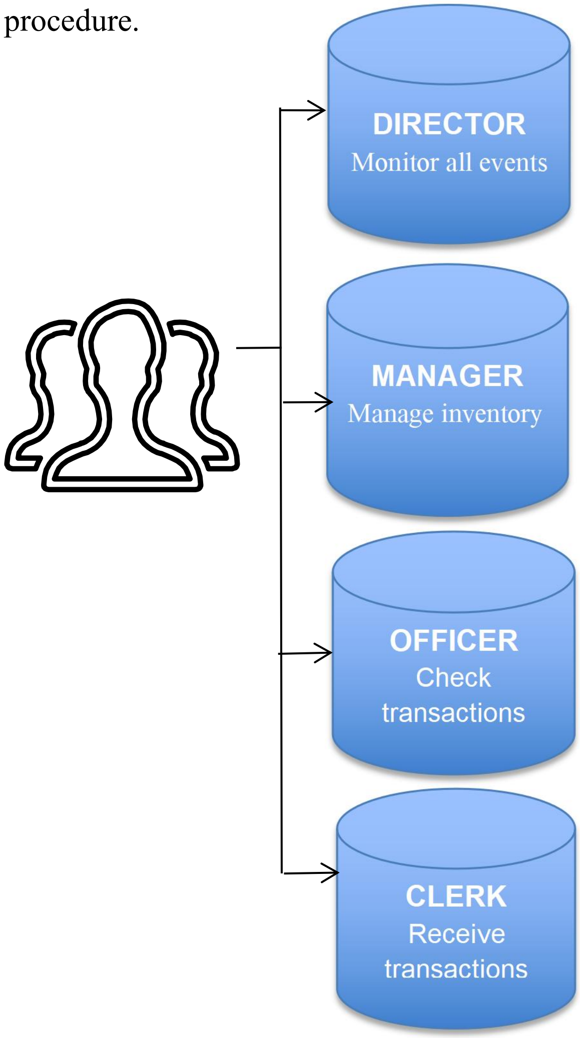


Fig.5. Categorizing users based on the different roles

Different users in a financial sector are being sorted and assigned different roles which differentiates them from one another. Regression analysis is also performed to verify the maximum probability of the rights provided to each investor. Comparing the roles of the preexisting user along with the new user, this system can easily identify the new entrant.

4) Private Block-chain:

The proposed system deals with private block-chain, also known as permission-based system. It is a block-chain network that operates in and is controlled by a financial jurisdiction. Access is granted only by invitation, and any capitalist wishing to use it must first obtain authorization from the governing body. The editing permission of every node is carefully regulated by the governing organization. Due to the lesser number of nodes a private block-chain can execute transactions significantly quicker and at a lower cost.

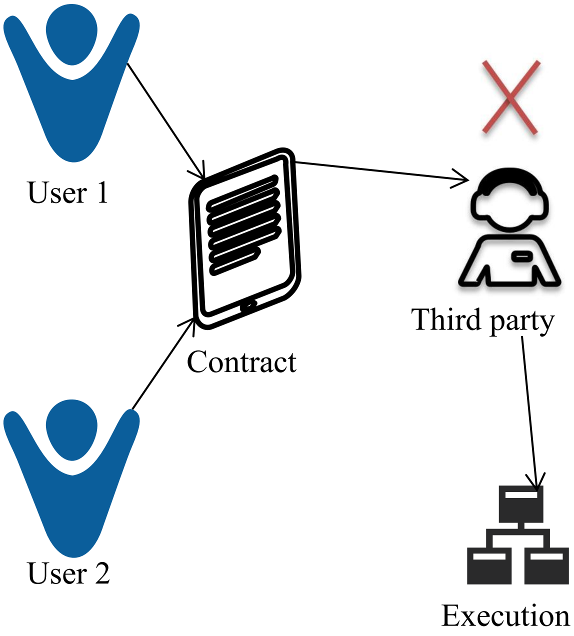


Fig.6. Smart contracts

The usage of Smart contracts which are electronic contracts that allow multiple anonymous parties to engage in an arrangement. They are tamper-proof computer programs that are not controlled by any central authority(third-party). SCs can reduce adversarial risk, boost efficiency, minimize costs, and add new levels of transparency to financial operations. The agreements make it easier to exchange currency, assets, resources, or any commodity, and this is how transactions are open, permanent, and identifiable.

IV. RESULTS AND DISCUSSION

IAM Solution and Services hold high prevalence in the current digital world, where security is always a concern given the nature and mode of transactions. Being able to detect unusual access and outlier forms is absolutely necessary for an organization in the financial firm to be able to address many of the challenges in each of the IAM's major areas. Having an outlier or risk based view with proper authentication, cryptographic data, segregation of user roles, non-privatized smart contract ensures secure contracts and negotiations between organizations in the financial industry.

V. CONCLUSION AND FUTURE ENHANCEMENTS

There are always some challenges and scope to improve the previous implementations in existing commercial businesses by introducing a new scalable network policy, maintaining a chained network, transaction cost, proper selection of consensus protocol, developing standards for taut architecture, analyzing security threats, and many other aspects.

Applications that are built must be partition resistant. In other words, the systems connected in a privatized network should be highly available and have redundant copies of data. The failure of a system may not lead to stumbling block rather the backup stored in the other system can be used to carry out the intended trading. This way, the waiting time and piggybacking can be avoided using strongly secured applications.

VI. REFERENCES

[1] Md. Rayhan Ahmed, A. K. M. Muzahidul Islam, Swakkhar Shatabda, Salekul Islam "Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey" (2022) Available online: https://ieeexplore.ieee.org/document/9927415

[2] Jayanth Rama Varma "Blockchain in Finance" (2019) Available online: https://journals.sagepub.com/doi/pdf/10.1177/0256090919839897

[4] Ion-Petru, Cătălin Alexandru, Mădălina Ecaterina "Identity and Access Management - A risk based approach" (2015) Available online: http://conference.management.ase.ro/archives/2015/pdf/62.pdf

[4] I.Indu, P.M. Rubesh Anand, VidhyacharanBhaskar "Identity and access management in cloud environment: Mechanisms and challenges" (2018) Available online: https://www.sciencedirect.com/science/article/pii/S2215098617316750

[5] Soonduck Yoo "Block-chain based financial case analysis and its implications" (2017) Available online: https://www.emerald.com/insight/content/doi/10.1108/APJIE-12-2017-036/full/html