

CSE 543: Information Assurance and Security

Arizona State University, Fall 2022

FINAL PROJECT REPORT - Group 2-1

PROJECT TITLE:

Provisioning and De-provisioning for Identity Management in Cloud Computing from Service Provider's Perspective Using Blockchain and Machine Learning

GROUP MEMBERS:

ASU ID	NAME	EMAIL ID	ROLE
1222119366	Akash Roshan Mund	armund@asu.edu	Group Leader
1222272948	Bhavani Priya Kuche	bkuche@asu.edu	Deputy Leader
1225368924	Amey Bhilegaonkar	abhilega@asu.edu	Member
1222124176	Rohit Vishwanath Badugu	rbadugu@asu.edu	Member
1225565796	Naveen Aaditya Chitirala	nchitira@asu.edu	Member
1224246933	Kasi Kishore Ravuri	kravuri@asu.edu	Member
1223073865	Mahita Singamsetty	msingams@asu.edu	Member

Table of Contents

1.0 Introduction	3
1.1 Motivation and Background	4
1.2 Goals and Scope	5
2.0 Summary	6
3.0 Accomplishments	8
4.0 Detailed Results	11
4.1 Why Provisioning and De-provisioning	13
4.1.1 What is Provisioning and Deprovisioning User Access in IAM?	13
4.1.2 What are ideal cases where Provisioning and Deprovisioning is useful?	14
4.1.3 Benefits	14
4.1.4 Provisioning	14
4.1.5 Deprovisioning	12
4.2 Approaches for Provisioning And De-Provisioning	16
4.2.1 Advantages of Automated Provisioning and Deprovisioning	18
4.3 Service provider problems	19
4.4 Manual provisioning and disadvantages	20
4.4.1 Manual Provisioning	20
4.4.2 Disadvantages of manually provisioning and de-provisioning	22
4.5 Why Machine Learning for provisioning	23
4.6 Machine Learning advantages for provisioning and deprovisioning	25
4.7 Why Blockchain for provisioning and deprovisioning	27
4.8 Blockchain Smart contracts for provisioning and de-provisioning	31
4.8.1 Approach	31
4.8.2 How does smart contract work	33
4.8.3 System Architecture	34
4.8.4 Protecting blockchain from attack	34
4.9 Blockchain advantages for provisioning and deprovisioning	36
4.10 Blockchain disadvantages for provisioning and deprovisioning	38
4.11 Azure Active directory	39
4.11.1 Provisioning/Deprovisioning using Azure Active Directory	39
4.11.2 Limitations	41
4.12 AWS Fraud detection	42

4.12.1 What's the solution?	42
5.0 Conclusion And Recommendations	45
5.1 Conclusion and Recommendations for Blockchain	46
5.2 Conclusion and Recommendations for AWS fraud detection	46
6.0 References	48
6.1 Websites	50

1.0 Introduction

1.1 Motivation And Background

With today's increasing computing complexity and increased security concerns, users no longer feel safe even with a secure login and password. Identity management systems nowadays typically include biometric information, artificial intelligence, and machine learning, as well as risk authentication [2]. The globe is witnessing a rise in data breaches and the breaches can be prevented by utilizing technologies like Blockchain and Machine learning. Provisioning could be a key feature of the computing models, which provided guidelines to how users can obtain cloud services and resources from the service providers. As a consequence of rapid digitization and emerging technologies, the applications of machine learning have scaled up massively. Another emerging technology that has drawn attention as the future era's financial technology due to its security is Blockchain.

One of the first actions a business takes after hiring a new employee is to record that individual. Then, it falls to HR, IT, or a combination of the two teams to give the employee access to all of the programs, accounts, and systems they require to do their duties. As a result, user provisioning happens anytime data is added to or modified in your company's HR systems, which may happen as a result of, among other things, the addition of team members, changes to roles or promotions, or department transfers. In other words, user provisioning enables you to grant the appropriate amount of access to the appropriate users at onboarding, to update access during employment, and to remove access during the deprovision process when an employee departs the company.

The security issues in the domain of provisioning/deprovisioning user access in identity management on cloud computing and providing a solution using blockchain and machine learning are identified widely. So, by using machine learning and blockchain, the above mentioned issues are handled which we will be exploring in our project.

1.2 Goal And Scope:

In this project, from the service provider perspective, we will focus on security issues related to Identity management in provisioning and de-provisioning for Identity Management from the service providers view. Networks that weren't built for external access are suddenly being accessed regularly by BYOD devices and from locations the corporate has no control over. Using techniques such as blockchain and machine learning we will secure role-based access control to enable provisioning, and improve functionalities like scalability, integrity, and reliability by automating the process.

The project was focused in

- Determining the steps to be followed in order to secure the cloud resources which account for provisioning and de-provisioning for Identity management
- Determining the measures for preventing data breaches for security in cloud computing
- Training the machine learning models to detect and mitigate the threats
- Understanding the Blockchain technology to ensure data security in order to maintain liability of Identity management
- Separating cloud application providers from data processing and data storage providers

2.0 Summary

- Identity management, usually referred to as identity and access management, is a set of regulations and tools to guarantee that only authorized people have access to technological resources.
- Different components of Identity management system are: A scalable, secure, and standards-compliant directory service for storing and managing user information, a provisioning framework, a directory integration platform, a system to create and manage public key infrastructure (PKI) certificates, run time model for user authentication, delegated administration model
- The process of establishing, updating, and removing user accounts in several applications and systems is known as user provisioning and deprovisioning. This access control procedure occasionally includes related data, like group memberships, user privileges, and even the groups themselves.
- Mainly there are two kinds of provisioning and deprovisioning i.e. manual and automated provisioning and de-provisioning
- Ad hoc manual provisioning takes place. IT receives a request from HR, usually by email or the helpdesk. The necessary permissions are then manually granted by an IT consultant. Any internally managed IT resource, including group memberships, file sharing, network folders, directory accounts, email accounts, and software licenses, is referred to as an entitlement.
- Disadvantages of manual provisioning: Cumbersome and costly compliance efforts, Hampering employee productivity of employees, Ghost accounts, Overpaying on licenses
- Automated user provisioning makes sure staff only have access to the apps they need, which keeps your business safe.
- Advantages of automated provisioning and deprovisioning are easily onboard and offboard employees, streamline user management across applications, Increase security and reduce cost
- Primary reasons for the security breaches are centralized target management, Improper management of network/application/data access, Insufficient process automation, Failing to plan for scalability, Lack of management training, Lack of scheduled access management auditing
- Machine Learning technologies are crucial to developing a successful IAM strategy and can help to avert many problematic circumstances.
- It supports Advanced Analytics, Precise Access Control, Breach Detection and Prevention, Automation and Flexibility, Increased Visibility, Going Beyond Compliance

- Reduces errors, Minimizes security risks, Simplifies the process of (de)provisioning of IAM, Optimize Transparency Across Users, Easily Scalable
- Blockchain technology enables users to construct and manage digital identities, By combining the following elements: Decentralized identifiers, Identity management, Embedded encryption
- Few use cases of blockchain in Identity management are Self Sovereign identity, Data Monetization, Data Portability
- Advantages of using blockchain for provisioning and deprovisioning: Outsourcing the access control process, Offering a versatile access control solution, Automation of the access control process, Allow for the implementation of new business models for network and service providers, Ease of obtaining duplicate id proof after losing the original, Lower transaction costs due to the cutting out of intermediaries, Falling prices because of greater market transparency
- Azure Active Directory is a single sign-on, multi factor authentication, and conditional access business identity solution that offers protection against 99.9% of cybersecurity assaults.
- Customers may identify potentially fraudulent actions and capture more online fraud faster with the aid of Amazon Fraud Detector, a fully managed service founded on Amazon's knowledge from more than 20 years of operation.
- A smart contract is a program that runs on the Ethereum blockchain. It is a set of code (its functions) and data (its state) stored at a specific address on the Ethereum blockchain. Smart contracts are an Ethereum account type. This means they have a balance and can be a transaction target. They are not, however, controlled by a user; rather, they are deployed to the network and run as programmed.
- User accounts can then interact with a smart contract by submitting transactions that execute a smart contract-defined function. Smart contracts, like regular contracts, can define rules and automatically enforce them through code. Smart contracts are inherently irreversible and cannot be deleted by default.
- A smart contract can be written by anyone and deployed to the network. All you need to do is learn to code in a smart contract language and have enough ETH to deploy your contract. Because deploying a smart contract is technically a transaction, you must pay Gas in the same way that you would for a simple ETH transfer. However, the gas costs for contract deployment are significantly higher.

3.0 Individual Accomplishment

Akash Roshan Mund [Leader]

- Compiled and Organized Project outline
- Compiled and Organized Final Report
- Research on Identity Access Management
- Research on Provisioning and Deprovisioning
- Completed Summary
- Completed Section 1.1
- Completed Section 1.2
- Completed Section 3.0
- Completed Section 4.2
- Completed Section 5.1
- Completed Conclusion and Recommendations
- Reviewed And Formatted Final Report

Bhavani Priya Kuche [Deputy Leader]

- Research on provisioning and deprovisioning in Identity Access Management (IAM)
- Leveraging Blockchain
- Research on Blockchain Applications in provisioning and deprovisioning in IAM
- Research on challenges and future trends for Blockchain in Identity Management
- Completed Section 1.2
- Completed Section 4.8.1
- Completed Section 4.8.2
- Completed Section 4.8.3
- Completed Section 4.8.4
- Completed Section 5.2
- Reviewed and Formatted final report

Amey Bhilegaonkar

- Leveraging Machine Learning Research
- Research on Identity Management with Machine Learning
- Research on Identifying Fraud Detection Using ML
- Research on Machine Learning Methods for Provisioning And Deprovisioning In IAM

- Compiled the results obtained from Machine Learning methodologies
- Completed Section 4.1.1
- Completed Section 4.1.2
- Completed Section 4.1.3
- Completed Section 4.12.1

Rohit Vishwanath Badugu

- Research on Problems Related To Provisioning And Deprovisioning In IAM
- Research on SCIM
- Research on Azure Active Directory
- Completed Section 4.4.1
- Completed Section 4.4.2
- Completed Section 4.11.1
- Completed Section 4.11.2
- Completed Conclusion and Recommendations
- Formatted the final report

Naveen Aaditya Chitirala

- Research on Pros and Cons of Machine Learning And Blockchain
- Research on components of the Blockchain technology
- Completed Cover Page, Index Page And Reference Section
- Completed Section 1.1
- Completed Section 4.1.4
- Completed Section 4.1.5
- Completed Section 4.10
- Formatted the final report

Kasi Kishore Ravuri

- Research on Provisioning And Deprovisioning in Identity Access Management
- Research on Machine Learning Applications in IAM
- Completed Section 4.3
- Completed Section 4.5
- Completed Section 4.6
- Completed Conclusion and Recommendations

- Formatted the final report

Mahita Singamsetty

- Research on Leveraging Blockchain For Provisioning And Deprovisioning In IAM
- Research on the Issues faced Due to Provisioning and Deprovisioning of Access
- Research on the Existing solutions Leveraging Blockchain in Identity Management
- Completed Section 4.7
- Completed Section 4.9
- Completed Conclusion and Recommendations
- Formatted the final report

The diagram illustrates the Identity and Access Management Life Cycle as a continuous loop. At the center is a large blue circular arrow with the text "Identity and Access Management Life Cycle". Surrounding this central element are several key processes in yellow boxes: "Provisioning" at the top, "Authentication / Authorization" on the right, "Self-Service / Delegation" below it, "Password Management" further down, "Role & Application Access Management" below that, "Compliance (Identity Certification & Reporting)" at the bottom, and "De-Provisioning" on the left. The cycle is initiated by "Identity (Staff, contractors, Nurses, Doctors)" at the top left, which leads to "Relationship Starts". The cycle concludes with "Relationship Ends" and "Identity (Staff, contractors, Nurses, Doctors)" at the bottom left. Red arrows indicate the flow from the top identity box through the provisioning and authentication processes, and from the bottom identity box through the de-provisioning and compliance processes. A small icon of a person with a red 'X' over it is positioned between the "Relationship Starts" and "Relationship Ends" boxes, symbolizing the end of a relationship.

Identity and Access Management Life Cycle

Identity
(Staff, contractors, Nurses, Doctors)

Provisioning

Authentication / Authorization

Self-Service / Delegation

Password Management

Role & Application Access Management

Compliance
(Identity Certification & Reporting)

De-Provisioning

Identity
(Staff, contractors, Nurses, Doctors)

Relationship Starts

Relationship Ends

Identity and Access Management Life Cycle

Copyright Amerindia Technologies Inc.

A well-equipped IAM system should provide system administrators with appropriate resource management tools, allowing for simple application on-boarding, off-boarding, and modification. Each application should ideally be able to be customized individually with connecting entitlements, which are used to grant access requests for a set of access permissions within that application and can be added, removed, and disabled as needed within the organization. Furthermore, Roles can be used to group applications and entitlements and then assign them to a user based on her access requirements. One limitation of traditional solutions such as Active Directory is the inability to control users' access to applications outside of your environment.

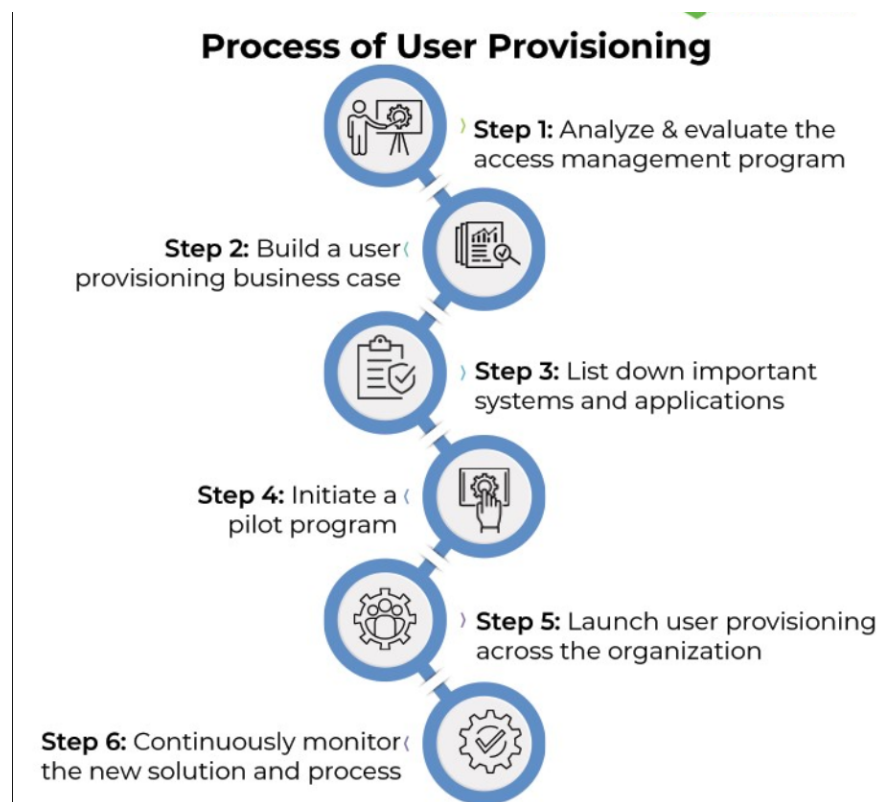
When a user's job description and title change, applications should be automatically deprovisioned by revoking access to a Role, and assigning a new appropriate Role should automatically provision the new set of applications and entitlements within the new Role. Regular account reviews and monitoring are required throughout the lifecycle of an identity, in addition to updating account privileges when known changes are required. These procedures should be carried out to ensure policy adherence, appropriate privileges, and accountability.

As an organization evolves, user accounts may be granted too many privileges at some point. This accumulation of access is known as "privilege creep" or "permission bloat." Regular reviews (i.e., "attestation and reconciliation" processes) allow for periodic evaluation and adjustment of privileges in accordance with the "Principle of Least Privilege." Account monitoring will assist in identifying any asset misuse or data security threats, ensuring that users who violate the organization's policies can be held accountable.

4.1 Why Provisioning and De-provisioning

4.1.1 What is Provisioning and Deprovisioning User Access in IAM?

The process of creating, updating, and deleting user accounts in several applications and systems is known as user provisioning and deprovisioning. This access control procedure occasionally includes related data, like group memberships, user privileges, and even the groups themselves. Automated user provisioning, which is the systematic creation and administration of user data in relation to users' capacity to access resources like apps that are available in one or more systems, has become popular in many organizations. Accessible systems may be cloud-based, on-premises, or a combination of the two. Every company should have a comprehensive identity management system for handling its identities effectively. It reduces the costs associated with identity management while also reducing the time and expense needed to meet employee requirements [1].



[Figure 2: Process Of User Provisioning](#)

4.1.2 What are ideal cases where Provisioning and Deprovisioning is useful?

Automated user provisioning is one of the main features of many identity and access management (IAM) solutions. Provisioning comes into play in the process called the joiner/mover/leaver (JML) process which is when an employee joins an organization, moves to a different department or division, or exits a company.

4.1.3 Benefits of provisioning and deprovisioning

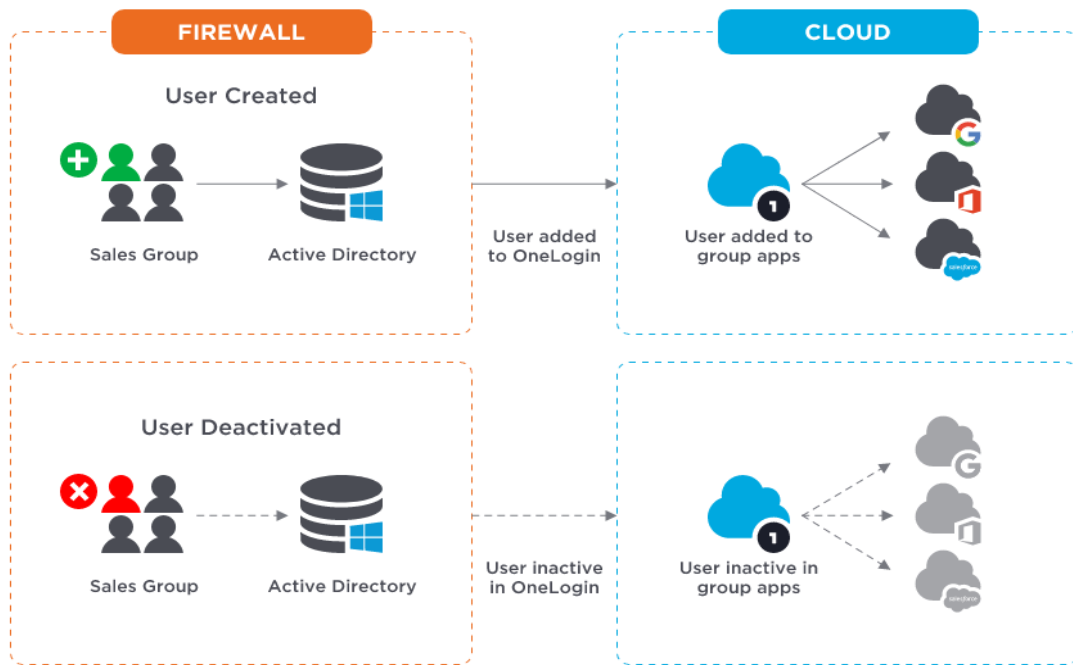
Easily onboard and offboard employees: Create and maintain employees' user attributes, such as usernames, roles, and profiles, and automatically assign access permissions and user accounts based on predefined roles and flexible entitlement rules. Streamline user management across applications: Automatically import users from Active Directory (AD), Lightweight Directory Access Protocol (LDAP), and other apps. Provisioning enables you to continuously propagate user profiles to ensure that your systems have the latest updates. Increase security and reduce cost: Use HR-Driven Identity Management (IM) to prevent former employees from having continued online access, to totally eliminate the possibility of zombie accounts sitting idle and at risk of being compromised.

4.1.4 Provisioning

In a fundamental automated provisioning procedure, users are added to apps in accordance with predetermined user roles. A user is immediately generated and given access permissions in the linked app once a role is assigned to that user. As shown in the diagram below, a newly created user is added to the Sales position and is subsequently given access to the apps related to that role after being deployed, in this case, the user who has been provisioned has access to G Suite, Office 365, and Salesforce.[3]

4.1.5 Deprovisioning

You want a solution that makes it easy to modify the user's status when it's time to deprovision former employees from apps so that all of their accounts will be terminated or suspended in accordance with the configuration choices you set. Using our scenario in the diagram as an example, after deprovisioning the user, the employee would no longer be able to access the apps related to their function.



[Figure 3: Provisioning Deprovisioning: One Login Blog](#)

4.2 Approaches for Provisioning And De-Provisioning

Businesses may make sure that the appropriate users have access to the necessary infrastructure and apps by using an identity provisioning system. Enterprises may use it to automate the providing and de-provisioning of all user accounts in a safe, automated, and policy-based manner. The central management of all application credentials is another feature of an identity provisioning system. In order to give solutions for expanding issue sizes in a suitable amount of time, scientific computing demands an ever-increasing number of resources[16]. The integrated provisioning engine establishes the entitlements of the user accounts and generates user credentials based on policies. While minimizing administrative effort, it swiftly links users to the right enterprise resources. The on-demand provisioning of services, which is a cloud-based extension for traditional service-oriented architectures, improves the handling of services in scenarios where they are only used rarely and irregularly.[12]

Cloud computing is a sophisticated system that combines a variety of networked devices to provide services that are in demand. Two computing resource provisioning options, referred to as reservation and on-demand plans, are available to cloud computing users from cloud providers[7]. A variety of flexible distributed systems with a wide range of connectivity and utilization make up the cloud computing architecture. Due to advantages including affordability, scalability, dependability, and flexibility, businesses are quickly embracing cloud networks. Cloud networks are susceptible to many types of network assaults and privacy concerns, despite the fact that the main benefits of cloud computing are encouraging realities. Identity and access management mechanisms are necessary in cloud environments due to characteristics like multi-tenancy and infrastructure that is maintained by a third party. Numerous scholars and members of the business have addressed the issues related to secure access to cloud resources. Since on-demand provided services fundamentally alter the nature of services, the conventional service selection method no longer applies[10]. In this project, from the service provider perspective, we will focus on security issues related to Identity management in provisioning and de-provisioning for Identity Management. In business applications, service orientation is a common paradigm that is becoming even more popular in the incredibly vibrant field of eScience.[9]

The processes of user provisioning and deprovisioning entail the creation, updating, and deletion of user accounts across a variety of applications and systems. These linked details, including user privileges, group memberships, and even the groups themselves, may occasionally be included in this access control approach. The joiner/mover/leaver (JML) process is what is involved in this. By directly connecting an IAM solution with HR and personnel systems, you may link user account creation, updating, and deletion

to HR activities. Permissions for accessing systems and apps connected to corresponding employee accounts may automatically change as a result of actions that affect HR data, such as those connected to employee onboarding and offboarding.

Currently many organizations are using manual provisioning and deprovisioning which comes with a cost such as If you manually manage people, you either have extremely labor-intensive, error-prone systems for regulating and recording who has access to what, or you don't. Furthermore, are you actually aware of when users' access to apps is given or denied? or if their privilege levels are altered?

You could incur very large charges for audit documentation if you don't have automated user provisioning and deprovisioning. The audit could be impossible for you to pass at all.

Deploying cloud apps in a large, globally dispersed business with several forests and domains in your Active Directory infrastructure might be difficult if you don't have a unified picture of all your users. Here manual provisioning and deprovisioning will become a bottleneck.

Deprovisioning users in a timely manner in order to avoid paying too much for application licenses is another problem for those utilizing manual techniques. The majority of cloud programs demand a yearly subscription for each active user. When you could just delete the old users and provide the seats to the new users, you could end up having to buy an upgrade in the midst of the subscription period if you neglect to remove inactive users from any of those apps.

When accounts are manually provisioned and deprovisioned, there is a chance that former workers or contractors might get access to them, either directly or through hackers who have their credentials. Few businesses have the proper procedures in place to make sure that when employees leave the firm, their cloud accounts are properly deleted.

The average cost of a data breach in the US is \$148 per record and \$7.91 million per breach, therefore firms who fail to provision and deprovision effectively or swiftly run a significant risk of expensive security breaches. Because of this, organizations that have had a large breach frequently underperform the market for years thereafter, and 60% of small businesses fail after a successful assault within six months.

4.2.1 Advantages of Automated Provisioning and Deprovisioning:

Hence, automated provisioning and deprovisioning plays an important role in the system. Active Directory and/or HR platforms like Workday may be easily synchronized using automated user provisioning. An employee's status as inactive is instantly recognized, and the person is deprovisioned from all of their cloud accounts. This essentially stops such users from gaining illicit access. Key benefits we get from automated provisioning and deprovisioning are

- **Easily onboard and offboard employees:** Create and maintain the usernames, roles, and profiles of your workers' user accounts, and use established roles and adjustable entitlement rules to automatically allocate user accounts and access rights.
- **Streamline user management across applications:** Import users automatically from apps that use LDAP, Active Directory (AD), and other directories. To make sure that your systems are up to date, provisioning enables you to transmit user profiles over time.
- **Increase security and reduce cost:** Use HR-Driven Identity Management (IM) to completely remove the potential of zombie accounts lying idle and at danger of being hacked. This will prevent former workers from having prolonged internet access.

In this project we are mainly aiming to increase the security of automated provisioning and deprovisioning using Azure active directory, AWS fraud detection and using the technology of smart contract in blockchain. We will discuss in detail about these technologies in next sections.

4.3 Service provider problems

Increasingly distributed workforce: One way for organizations to attract and retain top talent is to remove geographical constraints and provide a flexible work environment. A remote workforce allows businesses to increase productivity while lowering costs, as well as untether employees from a traditional office setting. However, with employees dispersed across a country or even the globe, enterprise IT teams face a much more difficult challenge: maintaining a consistent experience for employees connecting to corporate resources while maintaining security. Because of the rise of mobile computing, IT departments now have less visibility and control over employees' work practices.

Distributed applications: With the rise of cloud-based and Software as a Service (SaaS) applications, users can now access critical business apps such as Salesforce, Office365, Concur, and others at any time, from any location, and on any device. However, as the number of distributed applications increases, so does the complexity of managing user identities for those applications. Users struggle with password management without a seamless way to access these applications, while IT faces rising support costs from frustrated users.

Productive provisioning: Access must be manually provisioned by IT employees in the absence of a centralized IAM system. A user will be less productive the longer it takes for them to access essential business apps. On the other hand, failing to withdraw the access privileges of workers who have left the company or been moved to different divisions may have detrimental effects on security. IT staff have to promptly de-provision access to company data in order to close this window of exposure and risk. Unfortunately, this often requires IT to manually revoke access to resources by going through each user's account to determine what they have access to. Access provisioning and deprovisioning manually is a lot of work and is prone to mistakes or oversights. It is not an efficient or sustainable way to manage user identities and access, especially in large organizations.

Bring your own device (BYOD): To manage or not to manage—for today's businesses, there really is no choice. Employees, contractors, partners, and others bring personal devices into the workplace and connect to the corporate network for both professional and personal reasons. The challenge with BYOD is not whether external devices are brought into the enterprise network, but whether IT can react quickly enough to protect the organization's business assets without interfering with employee productivity and while providing freedom of choice. Almost every company has a BYOD policy that allows users to access secure resources from their own devices. However, using a mobile device to access internal and SaaS

applications can be more difficult than using a networked laptop or desktop as a workstation. Furthermore, IT staff may struggle to manage who has access to corporate data and which devices they use to access it.

Password problems: Because of the proliferation of cloud-based applications, employees must remember an increasing number of passwords for applications that may cross domains and use a variety of authentication and attribute-sharing standards and protocols. When an employee spends more and more time managing the resulting lists of passwords—which, for some applications, may require changing every 30 days—user frustration can mount. Furthermore, when employees have password issues, they frequently contact IT staff for assistance, which can quickly and repeatedly deplete critical resources.

Regulatory compliance: Concerns about compliance and corporate governance continue to be important factors in IAM spending. For instance, the IT department is mostly responsible for providing the corporate governance data mandated by Sarbanes-Oxley rules. It can be very helpful to reduce the burden of regulatory compliance and guarantee a smooth audit process if support is provided for procedures like identifying access privileges for specific employees, tracking management approvals for expanded access, and documenting who has accessed what data and when they did it.

4.4 Manual provisioning and disadvantages

4.4.1 Manual Provisioning:

Manual provisioning occurs on an ad hoc basis. HR submits a request to IT, typically by helpdesk or email. An IT specialist then manually provides the required permissions. An entitlement is any internally controlled IT resource, such as directory accounts, email accounts, network folders and file shares, group memberships and permissions, and software licenses. But this is merely the first step. Updates are required for promotions, transfers, terminations, new duties, and so on. When an employee leaves, IT must de-provision his or her rights. Furthermore, IT may be in charge of cyclical audits in which entitlements are examined for compliance, inventory, and monitoring objectives. This is frequently a 'rolling,' never-ending process.

But the consequences of skipping de-provisioning are considerably more harmful. The most frequent instance is permission creep. This happens as a result of employees' accounts gradually accumulating outdated permissions. Even worse, unused accounts may amass over time. If this buildup is left unchecked, former workers may continue to have access to their accounts for weeks, months, or even longer. This poses a serious danger to both compliance and security [9].

All of this adds to the workload already placed on IT personnel, who must also manage remote workers, fix outages, and advance new initiatives. Every action also reflects a possible error.

For instance, HR can neglect to inform IT of changes. Or, IT might not provide access to all necessary entitlements. When there is no automated mechanism in place, mistakes like this happen frequently. New hires could get trapped, unproductive, and unable to begin working on their first day.

Most organizations that manage users manually either reach a breaking point or are blissfully unaware of the danger. Organizations can save a significant amount of money by reducing manual processes while also closing a gaping security hole in their cloud IT footprint by leveraging automated provisioning and deprovisioning [14].

4.4.2 Disadvantages of manually provisioning and de-provisioning

Cumbersome and costly compliance efforts: Many businesses must follow federal or industry regulations, such as HIPAA (Health Insurance Portability and Accountability Act) or the Sarbanes-Oxley Act (SOX). They require organizations to have documented internal controls and processes in place to manage who has access to various types of information. These regulations also require that departing employees be deprovisioned as soon as possible so that former employees do not have access to systems. If you manage users manually, you either have time-consuming and error-prone processes in place to control and document who has access to what - or none at all.

Hampering employee productivity of employees: Modern organizations strive to make employees feel welcome and productive. Giving them access to the apps they require must happen quickly so that your new employees can get up and running as soon as possible. It's one way they know the company they've just joined is technically competent. And the work doesn't stop with new hires. Companies are constantly adding applications, and users' roles and responsibilities are constantly changing, necessitating the use of new applications. To keep users productive, you must be able to quickly grant them appropriate access to applications whenever they require it.

Ghost accounts: Manual provisioning brings the risk of unauthorized access to accounts from former employees or contractors; either from those individuals themselves or from hackers who have obtained their credentials. Few companies have the right processes in place to ensure that cloud accounts are effectively removed when people leave the company.

Overpaying on licenses: Another nightmare for those who use manual methods is deprovisioning users in a timely manner so that they do not overpay for application licenses. The majority of cloud applications have an annual fee per active user. If you fail to remove inactive users from any of those applications, you may be required to purchase an upgrade in the middle of your subscription term when you could simply remove the old users and give the seats to the new users. With automated user deprovisioning, you will always have enough headroom in your cloud to accommodate new users, allowing you to maximize your investment.

4.5 Why Machine Learning for provisioning

Machine Learning technologies are crucial to developing a successful IAM strategy and can help to avert many problematic circumstances. Artificial intelligence (AI) helps businesses transition from a completely technical approach to access control to one that is understandable at all organizational levels.

Advanced Analytics: With the use of artificial intelligence (AI), analytics may offer more precise and contextual information, enhancing the productivity of both technical and non-technical staff. The most recent technologies offer new ways to learn new information and automate procedures, which can greatly speed up the IAM compliance controls now in place. They can recognize fraud and other risks without the aid of security specialists. Employees are given the knowledge they need to choose wisely thanks to this. Such development is crucial, particularly in the areas of preventing insider threats and malicious detection. The organizations are continuously in charge, secure, and compliant in this way.

Precise Access Control: With the use of AI, it is simple to identify a user with additional protection utilizing sight and sound in addition to biometric passwords. AI would be able to recognize and confirm whether a person was who they claimed to be using visual and aural cues in addition to checking against predetermined credentials. Additionally, it might know when to allow access and take the appropriate action. Artificial intelligence (AI)-based access control is the logical progression from biometric ID. AI systems will also continuously watch out for any suspicious or fraudulent conduct carried out within the scope of a user's access privileges. It can even tell if a user is downloading more files than usual or trying to use a feature of the system that they normally wouldn't.

Breach Detection and Prevention: AI will continuously monitor user behavior to identify any signs of malicious intent or breach activity. Machines can process enormous volumes of data, examine it more quickly than even the most devoted IT crew can, and notify enterprises of any suspicious activities early enough to prevent fraud network compromise or data loss. By analyzing how various identities interact with enterprise networks, AI "learns" patterns of user behavior and incorporates them into security policies. This allows the system to distinguish between what is legitimate and usual and what is malicious or suspicious.

Automation and Flexibility: AI makes it simple to automate authentication and has the capacity to monitor minute details of user behavior for low-risk access circumstances, which lessens some of the IT department's administrative workload associated with IAM. IAM becomes effective and granular by

taking into account these factors before granting network access, which can prevent issues brought on by erroneous provisioning or de-provisioning. AI-powered solutions are able to apply appropriate IAM policies to any access request on the basis of requirements and conditions, eliminating the need for the IT department to waste time trying to determine the fundamentals of least privilege for each scenario.

Increased Visibility: For individuals in charge of identity administration, the concept of identity has expanded to encompass not only human users but also gadgets and programs. On a daily basis, a sizable number of identities with a diverse range of circumstances may access resources throughout a network of an organization. When flexible or remote workers are involved and cloud technology makes it possible for users to access networks from any location or device, the problem becomes even more complicated. The management of circumstances involving the addition of access by clients, customers, or other parties to the picture and the constant execution of IAM standards is becoming challenging, if not impossible, for IT teams. By using AI, everything is constantly monitored, and eventually a machine will be able to spot fraudulent activities. IT teams are able to create more intelligent administrative procedures and make more educated decisions about user permissions as a result of the network's complex interactivity becoming visible.

Going Beyond Compliance: Many businesses make the error of believing that adhering to security and privacy laws is enough to ward off hackers. Actually, these laws are insufficient to satisfy every organization's security requirements. The fundamentals of compliance involve limiting access to information to those who require it and disregarding everyone else. AI-powered IAM's adaptability and flexibility are highly useful in these circumstances. Enterprises confront less of a struggle when implementing security standards since AI and ML constantly monitor traffic, learn behaviors, and apply granular access limits, and it becomes challenging for hackers to utilize stolen credentials in any way.

4.6 Machine Learning advantages for provisioning and deprovisioning

Reduces errors: It might be difficult for IT personnel to enter a lot of onboarding data when a business is scaling. Human mistakes can occur throughout the manual data input process, which can result in lost time and money. The use of Machine Learning reduces the need for manual tasks like data entry and lowers the possibility of human error. Because automated provisioning requires less manual entries from IT personnel, such as onboarding data, the likelihood of errors is considerably decreased.

Minimizes security risks: Machine learning automates onboarding and offboarding in the identity management process and eliminates ineffective workflows. It keeps track of who has access to what platforms, programs, and information. IT workers can quickly create, modify, and remove accounts from the system and make sure the correct person has the appropriate permissions by using automatic provisioning. For instance, if an employee leaves a firm and the IT staff does not disable that employee's access to company systems, that employee may still be able to access company resources, creating a serious security risk to the business. The IT department can stop offloaded employee accounts from using business resources with the aid of automated provisioning. Security concerns are reduced as inactive accounts are deleted.

Simplifies the process of (de)provisioning of IAM: HR teams urge IT teams to develop profiles for new hires when they are employed. They also do other actions, such as giving employees access to apps and systems and providing user credentials. The IT staff's manual methods for adding responsibilities and creating profiles take time and cause delays.

Company A hires X. Before X first day on the job, an admin adds X to Cloud Identity by creating an account. The admin also adds X to an organization. X will be able to access the cloud apps assigned to that organization. Cloud Identity replicates X's identity to all of those cloud apps



[Figure 4: Cloud Identity replicates X's identity to all of those cloud apps](#)



[Figure 5: On the first day, X logs in to Cloud Identity](#)

Through SSO, X can access the cloud apps X needs using Cloud Identity credentials

By using an IAM platform for automated provisioning, manual processes are eliminated. The IAM provisioning and deprovisioning processes are automated. Identity creation and permission granting occur automatically without assistance from the HR or IT teams when a new employee is employed or a new application is added to the system.

Optimize Transparency Across Users: In the Identity and Access Management (IAM) platform, automated provisioning gives users access to tools and applications depending on their roles and permission levels. This provides administrators with a clear view of who has access and how they are using it, enabling them to modify permission levels as necessary. Automated provisioning offers a consolidated, connected view of user access and identities, in contrast to manual processes that lead to inefficiencies and a lack of transparency with tools used to provide and track access.

Easily Scalable: Because change is unavoidable in any organization, automated provisioning enables you to scale your IAM platform in lockstep with your business. By adding users to specific roles within your identity management solution and allowing the system to provision and de-provision tools and applications, automated provisioning aids in user lifecycle management. These automated processes help to streamline your IAM program by automating onboarding, offboarding, and overall identity lifecycle management.

4.7 Why Blockchain for provisioning and deprovisioning

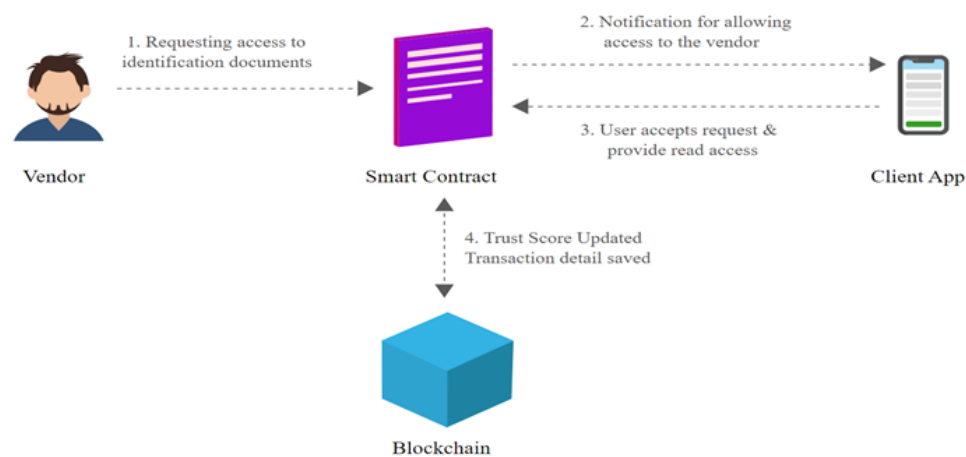
Personal data collection for business purposes is critical. On the one hand, when a user joins an organization and is promoted or transferred to another position or department, the employer's access should be revoked; if this does not occur, users lose control over the property of their data and are rarely aware of what they are sharing with whom. On the other hand, laws such as the European General Data Protection Regulation attempt to restore data control and ownership to users. In this paper, we discuss the potential impact of blockchain technology on the development of autonomous and resilient data management systems capable of ensuring data ownership and traceability. The application of this technology could play a significant role in the creation of a transparent global market of aggregated personal data in which voluntary acquisition is subject to clear rules and some forms of incentives, making the process not only ethical but also encouraging the sharing of high-quality sensitive data.

Many IT corporations' core business is the acquisition and processing of personal data via mobile applications and IoT devices. The amount of data generated is massive. Individuals now have little control over how their data is collected, viewed, and monetized. All major countries are likely to enact specific privacy laws to protect personal data in the future. The GDPR protects any information that can be used to identify a person, either directly or indirectly. This data ranges from usernames, emails, and IP addresses to healthcare information and bank account information. Laws such as the GDPR increase the security requirements of any business that processes personal data, resulting in increased burden and risk for the companies involved. Big IT corporations can manage the risk by delegating the collection and aggregation of personal data to new specialized companies. To control and trace the use of personal data, open networks and public ledgers can provide an alternative business model. The blockchain has the potential to lead to the development of independent and resilient data management systems capable of ensuring data ownership and traceability while also raising user awareness.

This may ensure more equitable data use, and it may be the only viable way to collect sensible data on a voluntary basis, such as healthcare-related information and biological profiles. Nonetheless, the adoption of a blockchain infrastructure has its own limitations, and the open issues are numerous. For example, in relation to the right to be forgotten, blockchain deletions or, more broadly, blockchain updates should be thoroughly investigated. The purpose of this paper is to look at the possibilities offered by this new technology in the development of new ways to collect, maintain, and use personal data, as well as to discuss some of the issues and limitations that must be overcome for it to be effective in this scenario. A blockchain infrastructure may be the best way to reclaim user ownership of their data. Users can be encouraged to share more personal and sensitive data with specific companies, even on a voluntary basis,

and can revoke such privilege at their discretion if they have a clear understanding of what is shared and with whom. Furthermore, this technology can provide the necessary infrastructure for the development of a global market for aggregated personal data: well-informed conscious users can choose to share their personal data voluntarily in the presence of clear usage rules and economic benefits.

summarizes previous research on the application of blockchain technology in the field of data provisioning briefly explains the key concepts underlying blockchain technology and the concept of network coalition investigates the concept of forming a network coalition to promote voluntary data provisioning. Blockchain was originally designed to record transactional data, which is relatively small, whereas the information to be stored can be large, for example, many images or treatment plans must be recorded in the healthcare domain. To address this issue, the concept of off-chain storage has been proposed in the literature. Essentially, data will be stored outside of the blockchain, in a traditional database, with the blockchain only used to store digital fingerprints to ensure data authenticity.



[Figure 6: Process of connecting to the blockchain with smart contracts for accessing required documents](#)

A blockchain is simply a chronologically ordered list of permanent data blocks. The genesis block is at the top of the list and contains some evidence about its release date, while each subsequent block is generated at regular intervals and contains a cryptographic message digest, or briefly a hash, of its predecessor, forming a chain of references. Each block also includes a proof of work, which is evidence that a certain amount of effort was expended in producing it. This proof is obtained by repeatedly applying a cryptographic hash function to a block, with each iteration varying its content by using a different nonce, until one of the target hashes is found. The described operation is part of the mining process that is ongoing at the same time. Changing a given block necessitates recalculating the hashes of all its descendants in a limited amount of time. Because such an operation can be quite costly, the

likelihood of seeing a block replaced by another one decreases over time as new ones are added in front of it. A block that refers to a given one is said to confirm it, and a block is considered practically immutable after a certain number of confirmations. The blockchain technology's key innovation is a decentralized emergent consensus protocol that allows a group of agents to reach an agreement about a global state by accepting data transmitted across an open byzantine Peer-to-Peer (P2P) network. Because agents can be self-interested, enter and leave the system without authentication or secure connections, and act strategically against the P2P protocol, the consensus can be considered emergent.

Blockchain technology is renowned for its security. Due to the lack of a centralized location from which cybercriminals may take data, information kept on the blockchain is impenetrable to cyber-attacks that often occur with centralized databases [22]. Decentralization, or the lack of an established central authority, is a key feature, as is the ability to have a dynamic composition, which means that new components can freely join the coalition while existing ones can leave. Governance rules are encoded within a set of smart contracts, and members hold a certain number of tokens that allow them to vote.

Data Provisioning Coalitions on a Voluntary Basis A blockchain infrastructure may be the best way to reclaim user ownership of their data. Users can be encouraged to share more personal data with specific companies, even on a voluntary basis, and can revoke such privilege at their discretion if they have a clear understanding of what is shared and with whom. The current process in user data provisioning is represented. This technology can also provide the necessary infrastructure for the development of a global market for aggregated personal data: informed and conscious users can choose to share their personal data voluntarily in the presence of a clear benefit.

The utility of a single piece of personal data, on the other hand, is difficult to quantify, and its value is typically very low. The value of personal data can only increase after some aggregation and integration process, which is typically performed by third-party companies that collect data from users and resell the aggregated data.

The Blockchain's Role in Ethical Data Acquisition and Distribution of 5 datasets to other businesses The current provisioning process is depicted in which users share their personal data to an organization, depicted in the middle, which is responsible for aggregating such raw data and producing useful information, which is then sold to other organizations, depicted on the right. Users are unaware of how such data are processed by the middle organization and have no control over the nature of the organizations on the right and the use of these data. It depicts an innovative data provisioning paradigm inspired by the use of blockchain technology and the formation of a voluntary-based DAO. A blockchain infrastructure has the potential to cause a paradigm shift in the acquisition and aggregation processes. With the right technology, users can volunteer to collect and aggregate their personal data, resulting in valuable information. The coalition may sell such data to other organizations while retaining control over

their use and transfer. In the event of a dispute, the blockchain can be used as a tamper-proof log and as evidence in court. Companies, on the other hand, can externalize some data acquisition costs and reduce the risk posed by improper handling of personal data in accordance with existing privacy regulations.

The potential of emerging blockchain technology for developing self-sufficient and resilient data management systems capable of ensuring data ownership and traceability Blockchain technology is regarded as an enabling technology, that is, a technology that opens the design space to new innovative applications and even new ways of thinking about algorithmic solutions in which economic factors play a significant role. We believe that this technology will be useful in encouraging users to share their data even in more sensitive contexts, such as health care, as well as in creating a global market for aggregated personal data. Despite the advantages of using a blockchain infrastructure for data provisioning, its adoption has its limitations, and the open issues are numerous.

4.8 Blockchain Smart contracts for provisioning and de-provisioning

Although distributed ledgers' primary function is to store data related to user interactions, their capabilities allow them to provide more sophisticated functionalities. Smart contracts, software programs that define immutable rules as functions stored on the blockchain and can be executed on demand, were introduced as blockchain technologies advanced. Smart contracts can communicate not only with users but also with one another through message exchange. We compare existing smart contract interactions and design an architecture for asynchronous state consensus, a novel type of smart contract interaction that is required in applications but has received little attention.

4.8.1 Approach

The provisioning of resources starts when the employee joins the organization and de-provisioning takes place when the employee exits the organization. As the data related to an organization should stay within the organization, we use a private or permissioned blockchain in order to avoid the third party. The approach demands the creation of 3 internal groups. One is a group of managers who has the information related to all the employees in their team respectively and second is the group of all employees in the organization and the third group is the group of Hiring managers (HR) who approve/decline the requests raised by the managers. The group HR has an IT administrator representative. Only the managers can communicate with HRs. And the employees can raise requests to managers.

The HRs have the access to the private blockchain in order to add or delete or update the information regarding the employees. Let's consider 5 scenarios where the HR group will have to make changes to the smart contracts.

1. An employee joins the organization
2. An employee gets promoted
3. An employee gets demoted
4. An employee changes their department/ team
5. An employee exits the organization

An employee joins the organization: When an employee wants to join the organization, after the interview process the manager raises a request to the HR department after the onboarding, providing the information about the new employee and the team they are going to join. The HR department enters the data of the new employee and creates a block with the information and appends it to the blockchain. The block now contains the details about the employee along with his date and time of joining. We write the

smart contract solidity code with a logic where the date and time of joining equals the current time, and the respective block gets appended to the blockchain. Once, the block is ready to get appended after the smart contract execution, a consensus algorithm runs in order to get approval and validation by the system. Once validated the block gets appended to the blockchain.

An employee gets promoted: When an employee gets promoted, the manager of the current team raises a request to HR and provides an update on the effective date and time of the change in the position of the employee. The HR approves the request and then updates the smart contract, once the current time is equal to the effective date and time, the block of that particular employee gets updated and will be granted the required cloud resources according to the manager's request.

An employee gets demoted: When an employee gets demoted, the manager of the current team raises a request to HR and provides an update on the effective date and time of the change in the position of the employee. The HR approves the request and then updates the smart contract, once the current time is equal to the effective date and time, the block of that particular employee gets updated and will be granted the required cloud resources according to the manager's request.

An employee changes their department/ team: When an employee from a particular department/ team wants to change their team. The employee first raises a request to the manager of the current team, and after the manager approves the request, the manager raises a new request to the HR department. The HR department then sends the request to the new team manager. Once the approval is done, the HR goes ahead and updates the smart contract with the team change effective time and after the consensus algorithm execution, the block gets updated and the existing cloud resources of the employee gets revoked and the new team managers request for the cloud resources to the employee gets granted.

An employee exits the organization: When an employee leaves the organization, the manager raises a request to the HR, the HR enters the date of exit in the smart contract and once the smart contract gets executed the employee block gets updated to an inactive state.

In all the scenarios we can see that the employee communicates with the manager and the manager communicates with the HR department. There is no direct communication between HR and the employee which makes sure there is no scope for confusion.

4.8.2 How does smart contract work

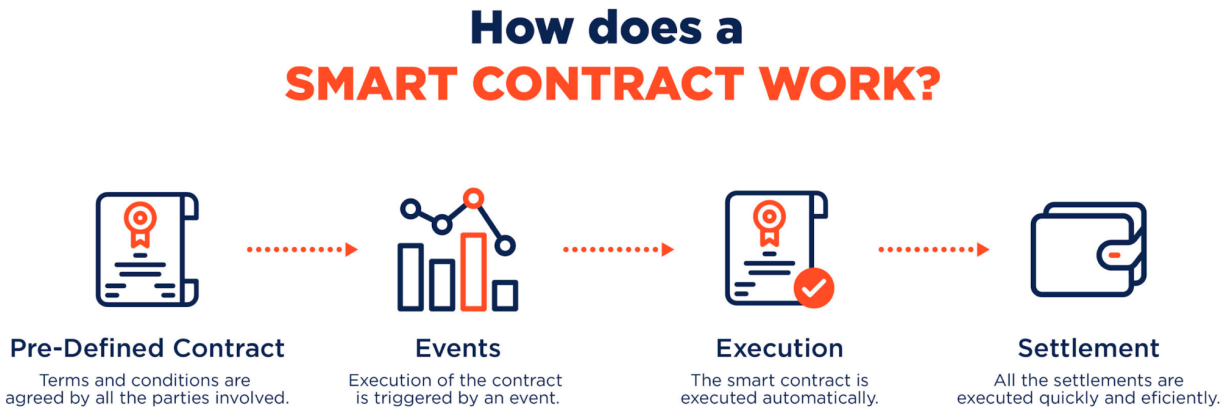


Figure 7: Smart contract operation

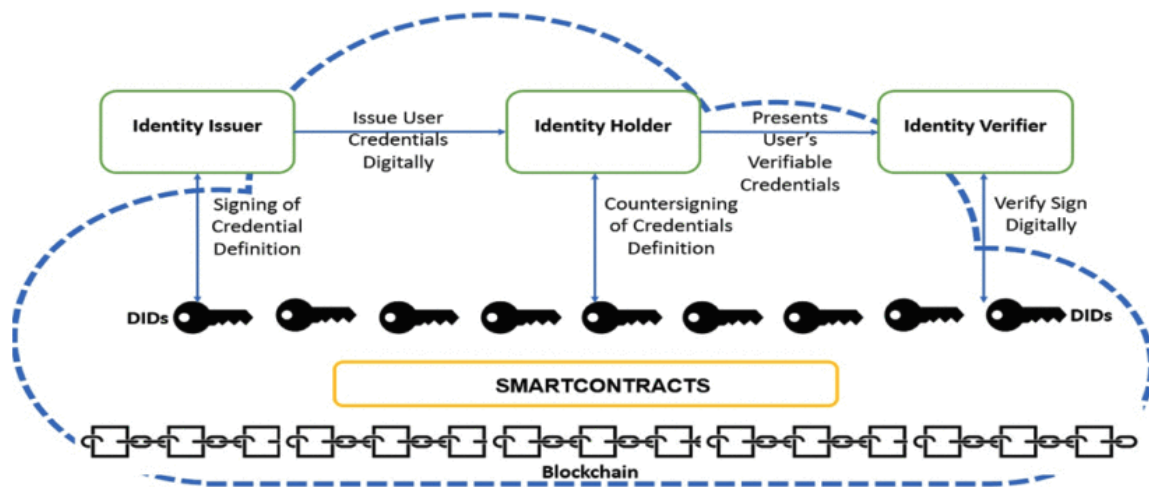
The benefits of DL technology and Blockchain are thought to be superior to legacy access control methods. Blockchain-Based Access Control (BBAC) can provide two distinct benefits. To begin, BBAC can impose a consensus mechanism for access control, allowing multiple stakeholders to control simulations. Decentralization could improve cloud security. Second, the time stamping and immutability of Blockchain entries can be used to improve governance and control capabilities for access control. [4] considered using a Blockchain-based system with a smart contract for the security of virtual machines (VM) and control over their access to the system's physical machines. Such access control aided in the prevention of threats arising from side-channel analysis and system attacks. For managing system access policies, Novo et al. [19] proposed a single smart contract-based system. The management hub concept was introduced to manage the many edge devices that have access to the blockchain network.

A blockchain has been used [6] in a decentralized access control mechanism to avoid single-point failure and possible misappropriation of secured and sensitive data by TTP. With blockchain technology as an effective access control mechanism, owners have complete control over access to their owned data. Using the decentralization method, Wang et al. [23] propose a Blockchain-based access control work that is capable of avoiding potential negative effects caused by untrustworthy third parties or users with questionable honesty. Nguyen et al. investigated the trustworthiness of access controls using Blockchain-based access control using medical records.

4.8.3 System Architecture

When using cryptographic credentials for cloud user authentication and authorization, four distinct steps are taken into account. First, cloud user identity and credentials must be registered. Second, retrieval and verification of identity credential-related information. Third, smart contract creation and deployment. Fourth, smart contracts are used to control and manage cloud resource access. Figure 1 depicts the overall system architecture. The proposed system includes a number of well-defined and specific modules that address the desired set of activities.

Furthermore, IAM actions are involved in identity transformation as triggered by Smart Contracts, identity access control, and, finally, identity verification. Identity transformation entails the use of hashing algorithms for secure transformation and storage retrieval. The smart contract's activation condition enforces the identity access control policies. Finally, as mentioned in the SSI verification process, identity verification is performed using a standard three-way verification mechanism.



[Figure 8: Issuing and verification of credentials in smart contract](#)

4.8.4 Protecting blockchain from attack

Organizations can take a few proactive steps to ensure their data is kept secure in the cloud.

As we all know, account hijacking is common among cloud computing network users. Even though the cloud owners/providers take all preventive measures, intruders find their way into hijacking the user

account. In order to protect our account from attacks the blockchain access holder has to make sure to follow the mentioned solutions.

- All sensitive information, such as credentials/passwords, should be thoroughly encrypted before being sent to the cloud.
- When possible, multi-factor authentication should be implemented. Users must enter static or dynamic passwords that are delivered via SMS, biometrics, hardware tokens, or other methods.
- The IP address space should be limited. Certain tools allow only specific IP ranges, ensuring that users access the firm's resources only through VPNs or corporate networks.
- In the event of data loss in the cloud, data backup must be done securely.
- For cloud-related apps, the authentication method must be strong.
- A protocol must be set up to securely share account credentials between employees and services.
- A method to understand the cloud provider's policies and SLAs before signing up for a cloud network. They can mitigate the consequences of exposing client account information and data leakage to external intruders. To ensure that the damage caused by the breach is contained, firms must be made aware of these techniques as well as common defense in-depth protection strategies.
- Proactive monitoring techniques should be used to detect unauthorized activity.

4.9 Blockchain advantages for provisioning and deprovisioning

1) **Outsourcing the access control process** to an entity without the need for a trusted third party. This feature has two advantages: first, it can reduce the service provider's processing load like access control, registration and second, no other organization is required as a trusted third party as it is a private blockchain, there is no third party

2) **Offering a versatile access control solution** smart contracts can be built to provide authorization options based on the needs of all parties. These requirements can take into account the needs of the network provider like how much the network provider will be paid, service providers like which service will be provided at what cost, and users like which service will be provided at what cost and for how long.

3) **Automation of the access control process:** there is no need for a central authority when smart contracts handle access control. Smart contracts can also make this process entirely secure, immutable, and automated.

4) **Allow for the implementation of new business models for network and service providers** instead of paying twice for the same service, in our proposed method, the user pays the service provider for its service, and the service provider is the entity that pays the network provider on the user's behalf in the following steps.

5) **Ease of obtaining duplicate id proof after losing the original** Because blockchain enables the permanence and tamper-proofing of records, the technology can assist here. Government agencies can use blockchain to store individuals' ID proof. This record is completely safe and reliable due to its tamper-proof nature, and the security features of blockchain ensure its permanence. If someone misplaces their original ID proof, government officials can easily issue a duplicate ID proof.

6) **Lower transaction costs due to the cutting out of intermediaries** Because of the reduction of middle people i.e intermediaries the costs are reduced and can be lowered as per the requirement and base expenses. The costs helps in the reduction of the inputs and considered the basic necessary items for the performance and implementation of the tasks. With block chain technologies the costs can be reduced with high security provision

7) **Falling prices because of greater market transparency** By all measures, blockchain outperforms any other record-keeping system in terms of security. Only with consensus on a blockchain network can the shared documentation of transactions be updated and/or modified. The information is only edited if all or a majority of nodes agree to update it. Furthermore, once a transaction is approved, it is encrypted and linked to the previous transaction. As a result, no single person or party has the ability to change a record.

Because blockchain is decentralized, no one has the right to update records at their leisure. Blockchain can be used to enforce stringent security in any industry that has a critical need to protect sensitive data, such as governments, healthcare, and financial services.

8) Efficiency increases Another aspect of the preceding point is auditability. Because each transaction is recorded in the blockchain for its entire lifetime, there is already an audit trail for you to see and check the authenticity of your asset. Businesses save a lot of money because blockchain eliminates the need for third-party intermediaries. You don't need anyone else to establish the rules and policies of exchange if you can trust your trading partner. The cost and effort spent on documentation and revisions is also reduced because everyone has access to a single, immutable version of the ledger.

9) Transactions are generally made more simple (documentation, contracts, payment) It is difficult to trace products back to their origins in complex supply chains. However, with blockchain, all goods exchanges are recorded, giving you an audit trail to learn where a specific asset came from. You also learn about every stop the product made on its journey, and this level of product traceability can help verify authenticity and prevent fraud.

10) Greater transparency thanks to decentralised data storage Transaction histories are now more transparent than ever before thanks to blockchain. All nodes in the network share a copy of the documentation because it is a type of distributed ledger. The data on a blockchain ledger is easily viewable by anyone. Everyone in the network can see the change and the updated record if a transaction history changes. As a result, everyone has access to all currency exchange information.

11) Flexible products (tariffs) and supplier switching Completing a transaction using traditional paperwork processes is exhausting because it requires third-party mediation and is prone to human error. Blockchain can streamline and discipline these legacy methods, removing the risk of errors and increasing trading efficiency and speed. Because there is only one ledger, parties do not need to maintain multiple documents, resulting in significantly less clutter. And when everyone has access to the same information, it is easier to build trust. Settlements can also be made smooth and easy without the use of intermediaries.

12) Privacy issues makes secured Data on a public blockchain is encrypted and anonymous, but it is accessible to all network nodes. As a result, everyone in the network has legal access to this information. Transactional data could be used to track down the identity of a person in the network, just as web trackers and cookies are commonly used by businesses. Unfortunately, this demonstrates that blockchain is not completely secure.

4.10 Blockchain disadvantages for provisioning and deprovisioning

1) Demographic Challenges: The demographic issues related to generating reliable digital IDs at scale are not sufficiently addressed by blockchain. A very diverse and difficult task is identity proofing and authenticating many demographics, such as students, elders, rural Americans, the homeless, millennials, and young professionals. Younger consumers frequently lack a financial history, may be included on their parents' utility account, and may lack a substantial government record-keeping history for the same reason.

2) Identity Verification: After an identity has been proven to be true and unique, the next problem is to confirm that the person claiming the identity is indeed the rightful owner of that identity and not a criminal. Identity verification is the next stage, and it is best carried out in person, such as during a trip to the state DMV, or online with strict controls applied in accordance with NIST 800-63-2 or -3 standards. The method is flawed even with these safeguards in place, and blockchain cannot prevent identity exploitation if a bad actor manages to take control of the identity of a genuine person because authentication and identity proofing take place upstream.[20]

3) Synthetic Identity: Establishing that the identity claimed is actual and distinct and the person claiming the identity is the lawful owner of that identity and not, for example, a member of organized crime is the most challenging task in identification. Regarding the first aspect of identity proofing, synthetic identity theft is a problem that blockchain cannot successfully address. This technique involves identity thieves combining a person's social security number, birth date, and address to construct a fictitious or "synthetic" identity. It is a ledger that records information but doesn't confirm or issue identities.

4) Immutability: The blockchain functions as an open, trustworthy ledger that relies on a decentralized network of nodes to check the accuracy of each transaction. A public blockchain theoretically provides a more democratic society in which transactions and the network itself are freed from centralized management. Unfortunately, the immutability of the blockchain does not hold in all the conditions.[21]

4.11 Azure Active directory

Azure Active Directory (Azure AD) is a cloud-based identity and access management solution.

This service enables your staff to access external resources such as Microsoft 365, the Azure portal, and thousands of other SaaS applications. Azure Active Directory also allows them to access internal resources such as apps on your corporate intranet network, as well as any cloud apps generated for your organization [11].

IT administrators use Azure AD to limit access to apps and app resources depending on business needs. You can, for example, utilize Azure AD to enforce multi-factor authentication when accessing critical organizational resources. Azure AD can also be used to automate user provisioning across your existing Windows Server AD and your cloud apps, such as Microsoft 365. Finally, Azure AD provides sophisticated features to help you automatically protect user identities and credentials while meeting your access governance requirements [18].

4.11.1 Provisioning/Deprovisioning using Azure Active Directory

The Azure AD Provisioning Service adds users to SaaS apps and other systems by connecting to the application vendor's System for Cross-Domain Identity Management (SCIM) 2.0 user management API endpoint. This SCIM endpoint enables Azure AD to add, update, and delete users programmatically. The provisioning service can also create, edit, and delete additional identity-related objects, such as groups and roles, for chosen applications. The provisioning connection between Azure AD and the application is encrypted with HTTPS TLS 1.2.

For automatic provisioning, the Azure AD provisioning service uses the SCIM 2.0 protocol. The service connects to the application's SCIM endpoint and automates the provisioning and de-provisioning of users and groups using the SCIM user object format and REST APIs.

Most applications in the Azure AD gallery provide a SCIM-based provisioning connector. Developers can utilize the SCIM 2.0 user management API to create a SCIM endpoint that interfaces with Azure AD for provisioning when creating apps for Azure AD.

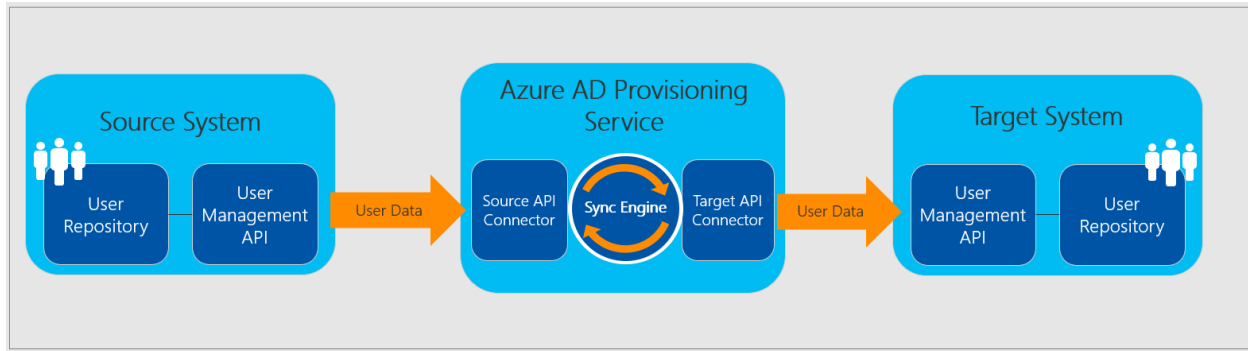


Figure 9: The Azure AD Provisioning Service

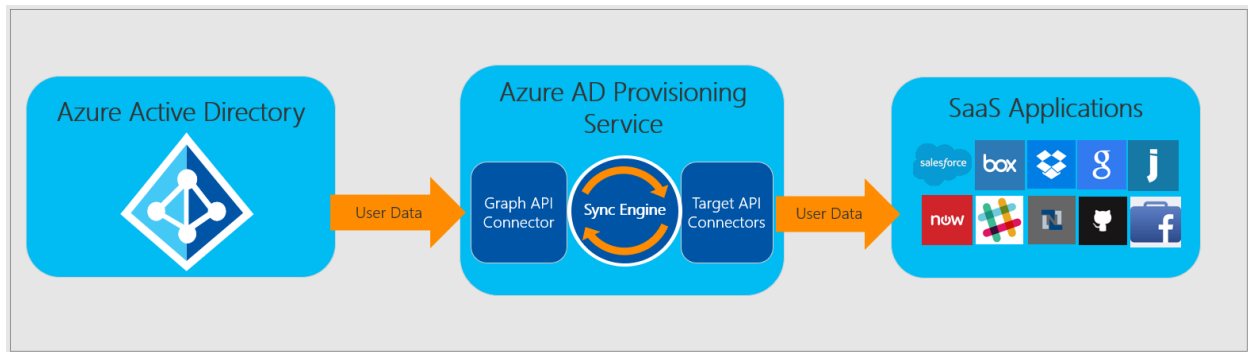


Figure 10: "Outbound" user provisioning workflow from Azure AD to popular SaaS applications

The Azure AD Provisioning Service adds users to SaaS apps and other systems by connecting to the application vendor's System for Cross-Domain Identity Management (SCIM) 2.0 user management API endpoint. This SCIM endpoint enables Azure AD to add, update, and delete users programmatically. The provisioning service can also create, edit, and delete additional identity-related objects, such as groups and roles, for chosen applications. The provisioning connection between Azure AD and the application is encrypted with HTTPS TLS 1.2 [14].

For automatic provisioning, the Azure AD provisioning service uses the SCIM 2.0 protocol. The service connects to the application's SCIM endpoint and automates the provisioning and de-provisioning of users and groups using the SCIM user object format and REST APIs.

Most applications in the Azure AD gallery provide a SCIM-based provisioning connector. Developers can utilize the SCIM 2.0 user management API to create a SCIM endpoint that interfaces with Azure AD for provisioning when creating apps for Azure AD [11].

By de-provisioning accounts when user access is terminated, the Azure AD provisioning service keeps source and target systems in sync. The provisioning service allows you to delete and disable users (also known as soft-deleting). The specific definition of disable and delete varies depending on the implementation of the target app, but typically, a disable signifies that the user is unable to sign in. A

deletion means that the user has been totally deleted from the application. In SCIM applications, a disable is a request to set a user's active property to false.

4.11.2 Limitations for Azure Active Directory

We shall send a disable request if a user previously managed by the provisioning service is unassigned from an app or from a group assigned to an app. The user is no longer controlled by the service at that time, therefore we will not issue a delete request if they are removed from the directory. Provisioning a disabled user in Azure AD is not supported. Before they can be provisioned, they must be active in Azure AD. When a user becomes active after being soft-deleted, the Azure AD provisioning service activates the user in the target app but does not automatically restore group memberships. The target application should keep the user's group memberships even when the user is inactive. If the target application does not support it, restart provisioning to change group memberships [17].

4.12 AWS Fraud detection

To define identity theft, the essential word here to consider is “identity.” Identity theft occurs when a criminal impersonates someone for the purpose of committing fraud, using the person’s private information such as a social security number or banking information. This could involve a situation where a loan is established under the individual’s name, or a falsified tax return is filed with the IRS, or a credit card is opened without the individual’s knowledge. While fraud is the result of identity theft, the big difference here is the implications upon the targeted individual. With identity theft, the damage to the individual is more severe. Unwinding the damage done by the fraudster can take months or years and can take a huge toll on credit scores.

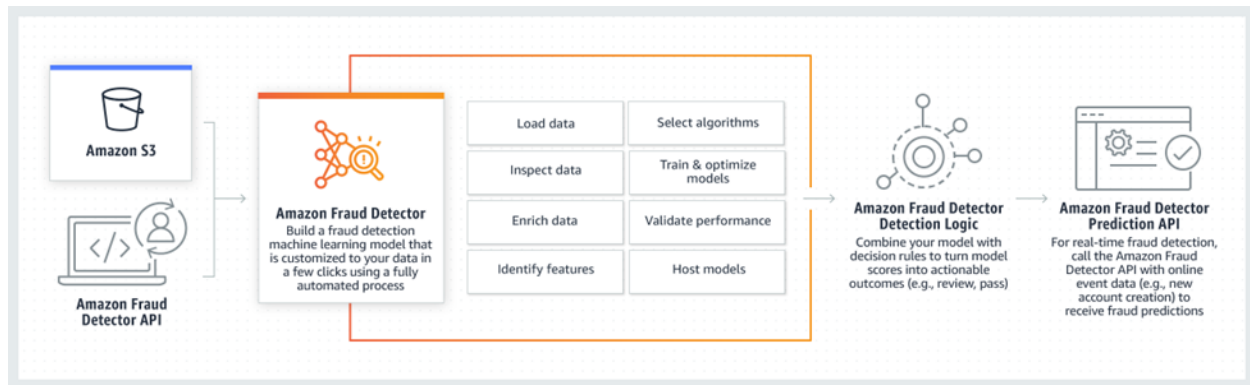
4.12.1 What’s the solution?

Amazon Fraud Detector is a fully managed service that makes it easy to identify potentially fraudulent online activities such as online payment fraud and fake account creation. Amazon Fraud Detector uses machine learning (ML) and 20 years of fraud detection expertise from Amazon Web Services (AWS) and Amazon.com to automatically identify potential fraudulent activity in milliseconds.

Some of more examples where Amazon Fraud Detection can be used:

1. New account fraud, within an account sign-up process
2. Online identity fraud
3. Payment fraud for online orders
4. Guest checkout fraud
5. Loyalty account protection






Amazon Fraud Detector automatically trains, tests, and deploys custom fraud detection machine learning models based on your historical fraud data, with no ML experience required. For developers with more machine learning experience, you can add your own models to Amazon Fraud Detector using Amazon SageMaker.



[Figure 11: Block Diagram: AWS Fraud Detection](#)

1. First, you define the event you want to assess for fraud.
2. Next, you upload your historical event dataset to Amazon Simple Storage Service (Amazon S3) and select a fraud detection model type, which specifies a combination of features and algorithms optimized to detect a specific form of fraud.
3. The service then automatically trains, tests, and deploys a customized fraud detection model based on your unique information.
4. During this process, you can boost your model performance with a series of models pre-trained on fraud patterns based on AWS and Amazon's own fraud expertise.
5. The model's output is a score ranging from 0 to 1,000 that predicts the likelihood of fraud risk. At the final stage of the process, you set up decision logic (e.g. rules) to interpret your model's score and assign outcomes such as passing or sending transactions to a human investigator for review.
6. After this framework is created, you can integrate the Amazon Fraud Detector API into you website's transactional functions, such as account sign-up or order checkout. A
7. Amazon Fraud Detector will process these activities in real time and provide fraud predictions in milliseconds to help you adjust your end-user experience.

Key features

				
Pre-built fraud detection model templates	Automatic creation of custom fraud detection models	Models learn from past attempts to defraud Amazon	Amazon SageMaker integration	Interface to review past events and detection logic

[Figure 12: Key Features of Amazon Fraud Detection](#)

5.0 Conclusion And Recommendations

Statistics show that companies that don't provision and deprovision effectively or fast run a significant risk of expensive security breaches. In the US, the average cost of a data breach is \$148 per record and \$7.91 million per breach. As a result, organizations that have had a big breach frequently underperform the market for years thereafter, and 60% of small enterprises fail within six months of a successful assault.

In the domain of Identity Access Management providing access to the user based on their requirement keeping in mind that the access is not excessive is one of the major problems every organization is facing. When a user is given more access than necessary for the tasks at hand, this is known as excessive permissions. An organization's volatility and complexity make it challenging to keep track of every user's permissions. Assigning and deleting rights may be challenging since each application and system may have its own unique permission model. The easiest method to reduce this risk is to only provide people access to what they actually need to carry out their tasks.

Further, managing employee permissions after they leave the firm is the other largest issue the IT department in an organization encounters. Any potential future security breaches against the firm will be avoided by implementing an end-of-life strategy for your gadgets. When an individual departs a business, make sure the IT department follows the same set of procedures.

Looking at the wide range of disadvantages of manual provisioning such as ghost account - which are one of the biggest threats to security, overdue costs due to excessive access to an employee, challenges on global deployment of cloud applications, time consuming compliance initiatives, we have decided to focus on the automated provisioning and deprovisioning in identity management system. But that comes with a cost of security threats due to excessive permission, misconfiguration, sharing data externally and onboarding and offboarding of employees. We mainly used three techniques to secure the provisioning of and deprovisioning in identity management. First one is using AWS fraud detection which aids consumers in spotting potentially fraudulent activity and speeds up the detection of more online fraud. Secondly we will be using Azure Active Directory which is a business identity solution that offers conditional access, multi factor authentication, and single sign-on to protect against 99.9% of cybersecurity threats. And lastly we are using blockchain smart contract technology. Simple blockchain-based programs called "smart contracts" that execute when certain criteria are satisfied. Usually, they automate the execution of a contract so that all parties may be confident of the conclusion right away, without the need for an intermediary or a delay.

Although cloud computing is incredibly cost-effective, adaptable, and dynamic, we need to be aware of its security concerns before implementing it. Identity management and access control are crucial to any security challenges. Using azure directory services, window azure has a good implementation of this technology. It is simple to combine these services. with the organization's typical active directory and offers a strong security framework for it.

5.1 Conclusion and Recommendations for Blockchain

Blockchain and smart contracts are game changers. This has the potential to alter various aspects of business. In this case, In our paper, we proposed a smart contract-based access control system. mechanism. The proposed method's high-level abstract in section 4.8.1. The primary goal of the proposed method is to provide a scalable and flexible access control system solution that does not necessitate the involvement of a trusted third party provider to outsource their access control requirements Our method also supports a new business model for lowering costs. the user's payment, improves access management automation, and eliminates the single point of failure (increasing the reliability). Access management with fault tolerance improves security. accountability, connection dependability, and addresses the requirements of the user, network provider, and service provider.

SECaaS for cloud-based systems is a viable option for ensuring cloud security. Among the factors examined in this work is IAM, which allows for a decentralized approach. This work also included cutting-edge security mechanisms in DID and Blockchain for secure web access for Cloud authenticated users. Its built-in time stamping feature is useful for system administration and control. Furthermore, such properties can be applied to time-stamped event logging and Cloud forensic applications. However, known flaws and vulnerabilities in Ethereum-based systems require special attention.

5.2 Conclusion and Recommendations for AWS fraud detection

Tens of billions of dollars are wasted on internet fraud globally each year. In the past, businesses relied on rule-based fraud detection programs, which aren't precise enough and can't keep up with fraudsters' evolving habits. Companies may proactively and more precisely identify and stop online fraud with the help of AWS Fraud Detection machine learning technologies. While adjusting to shifting threat patterns, these solutions will aid in lowering revenue losses, preventing brand damage, and delivering a frictionless online consumer experience.

While businesses with a dedicated team of data scientists can use Amazon SageMaker to develop highly specialized fraud detection solutions in days, businesses without a dedicated team of data scientists can use Amazon Fraud Detector to add ML-based fraud detection capabilities to their business applications in minutes.

The models that Amazon's Fraud Detection ML solutions develop are enhanced with knowledge of fraud tendencies thanks to Amazon's 20 years of expertise combating fraud and abuse at AWS, Amazon.com, and subsidiary businesses.

With Amazon's Fraud Detection Machine Learning solutions, customers can instantly apply containment or remediation measures intended to block or deny fraudsters and expedite low-risk activity to improve customer experiences for legitimate customers. These solutions score the risk of an event in real-time.

Amazon's Fraud Detection ML Solutions enable individuals who aren't machine learning experts but are familiar with fraud issues to participate in constructing and updating highly accurate models by automatically managing the complicated activities necessary to train, optimize, and deploy a fraud detection model.

6.0 References

- [1] E. Zavadskas, A. Kaklauskas, M. Gikys and N. Lepkova, "A multiple criteria decision support web-based system for facilities management", *International Journal of Internet and Enterprise Management*, vol. 2, no. 1, p. 30, 2004.
- [2] G. Goth, "Identity management, access specs are rolling along", *IEEE Internet Computing*, vol. 9, no. 1, pp. 9-11, 2005.
- [3] Becker, M., Drew, M. "Overcoming the challenges in deploying user provisioning/identity access management backbone". *BT Technol J* 23, 71–79 (2005). <https://doi.org/10.1007/s10550-006-0009-x>
- [4] Fongen, Anders. (2010). Identity Management without Revocation. 2010 Fourth International Conference on Emerging Security Information, Systems and Technologies. 75-81. 10.1109/SECURWARE.2010.20.
- [5] S. Ostermann, R. Prodan and T. Fahringer, "Dynamic cloud provisioning for scientific grid workflows", *GRID 2010*, 2010.
- [6] S. Czarnuch and A. Mihailidis, "The design of intelligent in-home assistive technologies: Assessing the needs of older adults with dementia and their caregivers", *Gerontechnology*, vol. 10, no. 3, 2011.
- [7] S. Chaisiri, B. S. Lee and D. Niyato, "Optimization of resource provisioning cost in cloud computing", *IEEE TSC*, vol. 5, no. 2, 2012.
- [8] H. A. Bheda and J. Lakhani, "QoS and performance optimization with VM provisioning approach in Cloud computing environment," 2012 Nirma University International Conference on Engineering (NUiCONE), 2012, pp. 1-5, doi: 10.1109/NUICONE.2012.6493187.
- [9] K. Vukojevic-Haupt, D. Karastoyanova and F. Leymann, "On-demand Provisioning of Infrastructure Middleware and Services for Simulation Workflows", 2013.
- [10] K. Vukojevic-Haupt, F. Haupt, D. Karastoyanova and F. Leymann, "Service Selection for On-demand Provisioned Services", *EDOC 2014*, 2014.
- [11] Zhang, Lan & Ning, Hong-yun & Du, Yun-yun & Cui, Yan-xia & Yang, Yang. (2016). Research on cross domain identity authentication in a federated environment. 1964-1968. 10.1109/CISP-BMEI.2016.7853040.
- [12] Karolina Vukojevic-Haupt; Santiago Gómez Sáez; Florian Haupt; Dimka Karastoyanova; Frank Leymann, "A Middleware-Centric Optimization Approach for the Automated Provisioning of Services in the Cloud", Feb 2016.
- [13] Mustafa Al-Bassam. "SCPki: a smart contract-based PKI and identity system". 2017 In: Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. ACM. 2017, pp. 35–40.

- [14] Yuanyu Zhang, Shoji Kasahara, Yulong Shen, Xiaohong Jiang and Jianxiong Wan, "Smart contract-based access control for the internet of things", *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594-1605, 2018.
- [15] Hamza, Kabiru & Gummi, Hassan & Yusuf, Mohammed. (2018). Identity and Access Management System: a Web-Based Approach for an Enterprise. Path of Science. 4. 2001-2011. 10.22178/pos.40-1.
- [16] Shangping Wang, Yinglong Zhang and Yaling Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems", *IEEE Access*, vol. 6, pp. 38437-50, 2018.
- [17] Syynimaa, Nestori. (2018). Who Would you Like to be Today?: Impersonation by Fake Azure Active Directory Identity Federation. 10.1109/TrustCom/BigDataSE.2018.00232.
- [18] Rini Mahajan, Dr. Manish Mahajan, Dr. Dheerendra Singh. (2018). "Window azure Active Directory Services for Maintaining Security & Access Control". International Journal of IT & Knowledge Management. Vol 11 Issue 2. pp:14-20
- [19] Oscar Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT", *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184-95, 2018.
- [20] Julija Golosova; Andrejs Romanovs , "The Advantages and Disadvantages of Blockchain Technology", November 2018.
- [21] Nursena Baygin; Mehmet Baygin; Mehmet Karakose, "Blockchain Technology: Applications, Benefits and Challenges", Nov 2019.
- [22] Sara Rouhani and Ralph Deters, "Blockchain-based access control systems: State of the art and challenges", *IEEE/WIC/ACM International Conference on Web Intelligence*, pp. 423-28, 2019.
- [23] Shangping Wang, Xu Wang, and Yaling Zhang, "A secure cloud storage framework with access control based on blockchain", *IEEE Access*, vol. 7, pp. 112713-25, 2019.
- [24] Fariba Ghaffari, Emmanuel Bertin, Noel Crespi, Shanay Behrad, Julien Hatin. A novel access control method via smart contracts for internet-based service provisioning. IEEE Access, IEEE, 2021, 9, pp.81253-81273. ff10.1109/ACCESS.2021.3085831ff.Ffhal-03245473f
- [25] Subbarao, D. & Raju, Bhagya & Anjum, Farha & Rao, Ch & Reddy, B.. (2021). Microsoft Azure active directory for next level authentication to provide a seamless single sign-on experience. Applied Nanoscience. 10.1007/s13204-021-02021-0.
- [26] Zhang, Mingming & Mao, Jiaming & Dai, Zaojian & Li, Yong & Zhang, Mingxuan & Fan, Lei & Xu, Liangjie & Hu, Jun & Wang, Anqi. (2021). The Cross-Domain Identity Authentication Scheme Has no Trusted Authentication Center in the Cloud Environment. 10.1007/978-3-030-78621-2_60.

[27] S. P. Otta and S. Panda, "Decentralized Identity and Access Management of Cloud for Security as a Service," 2022 14th International Conference on COMMunication Systems & NETworkS (COMSNETS), 2022, pp. 299-303, doi: 10.1109/COMSNETS53615.2022.9668529.

[28] Chowdhury, Mohammad & Noll, Josef. (2022). Integrated identity mechanism for ubiquitous service access'. IADIS International Journal on Computer Science and Information Systems. 2. 51-64.

6.1 Websites

1. [How Amazon Fraud Detector works with IAM](#)
2. [Build a fraud detection system with Amazon SageMaker](#)
3. [Amazon Fraud detection Block Diagram](#)
4. [How Amazon Fraud Detector Works](#)
5. [What is Amazon Fraud Detector](#)
6. [What is user provisioning and Deprovisioning?](#)
7. [Provisioning and Deprovisioning of cloud resources block diagram](#)
8. <https://sennovate.com/increasing-importance-of-artificial-intelligence-in-iam/>
9. <https://research.aimultiple.com/automated-provisioning/>
10. <https://identitymanagementinstitute.org/identity-and-access-management-challenges/>
11. <https://edtechmagazine.com/k12/article/2014/11/how-provision-and-deprovision-cloud-environm-ents>
12. <https://www.sailpoint.com/identity-library/what-is-automated-provisioning/>
13. <https://www.f5.com/services/resources/white-papers/the-challenges-and-benefits-of-identity-and-access-management>
14. <https://identitymanagementinstitute.org/identity-and-access-management-challenges/>
15. <https://edtechmagazine.com/k12/article/2014/11/how-provision-and-deprovision-cloud-environm-ents>
16. <https://www.sailpoint.com/identity-library/what-is-automated-provisioning/>