Implementing an IDaaS for Microsoft Active Directory using SensiPass Three-factor Dynamic Digital Signature

MSc Research project
Cybersecurity

Tushar Kaushik
Student ID: 19236158

School of Computing
National College of Ireland

Supervisor: Prof. Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Tushar Kaushik		
Student ID:	19236158		
Programme:	MSc Cybersecurity	**Year:**	2021-2022
Module:	MSc Internship		
Supervisor:	Prof. Vikas Sahni		
Submission Due Date:	07/01/2021		
Project Title:	Implementing an IDaaS for Microsoft Active Directory using SensiPass® three-factor Dynamic Digital Signature		
Word Count:	…6162…	**Page Count**…	22

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Tushar Kaushik

Date: …06/01/2022…

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Implementing an IDaaS for Microsoft Active Directory using SensiPass® Three-factor Dynamic Digital Signature

Tushar Kaushik
19236158

Abstract

Non-textual authentication procedures have been proposed throughout the previous two decades, as text-based authentication has been criticized. Non-textual authentication is potentially faster and more reliable, and it also presents a new paradigm for authentication decision-making. In this paper, the SensiPass® secure three-factor dynamic digital system had been extended using a new API for Microsoft Azure Active Directory. Integration of an IDaaS like SensiPass® with a market leader like Microsoft Azure Directory can open a gateway of opportunities for clients to secure their environment. Microsoft Azure's Conditional Access Policy works after the first factor of authentication is completed. The intention with conditional access policy is not to be the first line of defence for attacks like Denial-of-Service attacks. In the later part of the paper, a comprehensive analysis of various types of attacks, protocols, features, and different cloud identity management and their providers was done. Also, a network diagram was proposed for the new architecture.

1 Introduction

According to (Sharma, Sharma and Dave, 2015), IAM is a resource access management solution that involves user verification and permissions based on protective systems and the user's role. Identity and Access Management (IAM) is a mechanism for providing sufficient protection for an organization's systems and data by implementing rules and policies on users through various tactics such as applying login passwords, allocating privileges to users, and creating user accounts. IAM is constructed with two main building blocks which are Access management and identity management. Identity management is mainly concerned with identity provisioning and de-provisioning. Authentication, authorisation, and policy management are all part of Access Management. IAM oversees the permission to access which resources and when. IAM is also in charge of the user identity cycle, which involves user credential creation, maintenance, updating, and deletion.

(Tanwar, Tyagi and Kumar, 2019) says that, in a computer system, Identity and access management (IAM) consists of security architecture, tools, and technologies that are used to restrict access to vital data resources to genuine users in the appropriate context.

How well the users are authenticated, and the security of the credentials has a big impact on the security and integrity of a firm's assets and facilities. Criminals target these credentials, try to get hold of them, forge them, and get access to the user's systems to harm them. As per the National Institute of Standards and Technology (NIST), the mechanism through which our digital identity is authenticated is divided into three factors:

- Tokens (Physical objects which are unique)
- Biometrics (Physical characteristics unique to an individual)
- Secrets or knowledge factors

It is simple to steal or replicate these factors when they're used separately. These three factors are combined by SensiPass® into a single dynamic digital signature-based authentication system. With insider attacks posing a growing threat to vital infrastructure, we can no longer afford to defend our essential resources with merely two-factor authentication. With SensiPass® there is presented a unique innovation in the domain of authentication where humans are being authenticated. When SensiPass® is registered on a smartphone, Physical device attributes are captured and registered, and a token ID is created, and a highly secure three-factor digital dynamic signature is realised by fusing the device token with a biometric signature by using a secret interaction. Through this technology credentials sharing by employees and theft of identity by criminals both are made impossible. Credential database's vulnerability to theft and replay attacks are also eliminated through this method.

SensiPass® helps stakeholders to hold people accountable while accessing important assets and systems by facilitating proof-positive, end-to-end identity assurance, thereby dramatically decreasing fraud and insider threats. Understanding a user's behaviour in context is critical to verify a real person's identity. SensiPass® accomplishes this by building a contextual data cube around their behaviours and with the help of proprietary algorithms correlates their actions.[1]

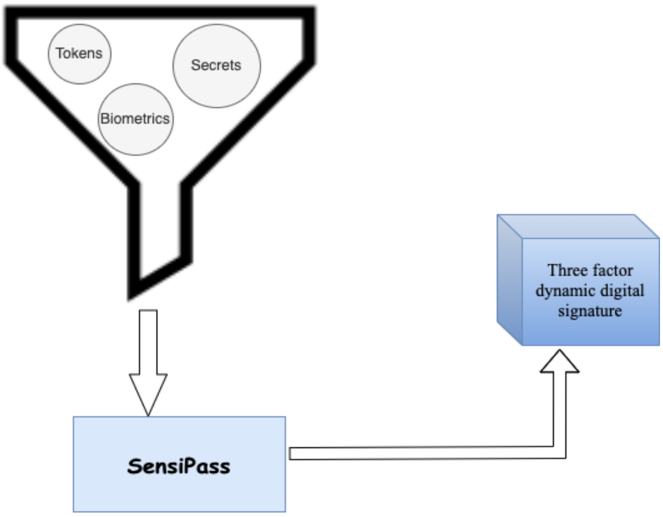


Figure 1. SensiPass® authentication workflow

[1] https://www.sensipass.com/why

Active Directory: Active directory is considered as a central data repository of all resources which are present in an organisation's network which include users, groups, devices, programs, and documents. It is adopted as a primary mechanism for managing data in most of today's significant enterprises.[2]

Azure Active Directory: Azure offers a broad range of services including security, virtual networking, communication mechanisms, and caching tactics in addition to computation and storage. Azure AD is primarily used as a cloud service providing web application authentication, single sign-on, and user management. Users for Azure Active Directory can originate from a range of locations. The first approach is Azure AD-based users, which entails manually creating users in the directory. The second option is to use a tool known as Azure AD Connect to synchronize user profiles from on-premises AD or Windows Server AD. [3]

SAML: According to (Hughes *et al.*, 2005) the Security Assertion Markup Language (SAML) protocol establishes a framework for securely transferring data among online business partners. Typically, SAML is an XML framework that allows entities to exchange security assertions. (Saklikar *et al.*, 2007) says that SAML has shown to be a nearly complete standard that does not require frequent changes to accommodate diverse Federation scenarios. An asserting party, also called as a SAML authority, is a system unit that produces SAML assertions, while a relying party is a system unit that relies on received assertions. Because it is seeking information from a SAML authority, the relying party is frequently referred to as a SAML requester.

2 Related Work

Three-factor authentication mechanisms and protocols have increased in popularity in recent years, combining passwords, smart cards, and biometrics to provide a much higher level of security than typical two-factor authentication, which relies on a password and a security token. There is currently a substantial quantity of literature on three-factor authentication for delivering safe authentication in a variety of use scenarios. The works of literature listed below demonstrate several security approaches for IoT-based networks, Wireless Sensor Networks, and other Cloud Computing applications.

2.1 Multi-factor authentication based on Biometrics

According to the NIST framework, three-factor authentication must be achieved through the following factors (i) Something you know, (ii) Something you have, or (iii) Something you are. (Kennedy and Olmsted, 2017) followed a different approach for three-factor authentication has been taken which is based on a password, username, and facial recognition through a mobile

[2] https://csrc.nist.gov/glossary/term/multi_factor_authentication
[3] https://core.ac.uk/download/pdf/326729493.pdf

phone. This approach uses a username and password as two different factors which would be considered as a single factor in the authentication process.
(Huang *et al.*, 2011) talks about a method for the authentication of clients with the help of three distinct methods, namely: Passwords, Smart cards, and biometrics. To upgrade two-factor authentication to three-factor a secure and generic framework had been proposed in this. The solution proposed by them is quite good, but the drawback is in the full identification of the practical threat.

As mobile devices are trending more and more amongst individuals at a fast pace which includes the fast exchange of sensitive information. Therefore, protection of the device is the need of the hour. There are multiple ways to do it, but face and iris recognition is better than fingerprints as they only need the device camera whereas fingerprints would require an additional dedicated sensor. (De Marsico *et al.*, 2014) talks about one such technique called FIRME (face and Iris recognition for mobile engagement). Separate and interchangeable packages are included in the architecture. It begins with acquiring the image. After that, for every distinct face and iris, various branches conduct segmentation, detection, feature extraction, and matching separately. However, when it comes to face recognition it is not completely safe as a further step for anti-spoofing should be added.

(Bhargav-Spantzel *et al.*, 2007) introduced two ID-based password authentication techniques that leverage passwords, smart cards, and fingerprints for the authentication of users. However, (Goldwasser, Micali and Rackoff, 1989) showed that after passively eavesdropping on only a single genuine login attempt, a passive eavesdropper can effectively login into the server without having no access to the password, fingerprints, and smart card.

(Li and Hwang, 2010) proposed different ways for tying a cryptographical generated key to a user's biometric template which would be kept in a database. The cryptographic key cannot be exposed without valid authentication of the biometrics. On the other hand, the client's privacy might be in jeopardy due to the biometric database.

2.2 Multi-factor authentication based on Cloud Computing

According to (ALSaleem and Alshoshan, 2021) many popular web services such as Azure, google provides multi-factor security as an optional feature that is deactivated by default. Many security techniques such as shoulder suffering, anti-capturing the screen are proposed. Suppose even if the hacker exposes the username or password by any means, it will be very tricky for the hacker to get inside the system as we would have to know and surpass all the authentication factors. Apart from the username and password, a third feature called PC ID has been added. This feature makes it impossible for a user to log in from a different system if the admin has not added him to a whitelist. At the time of registration, the user needs to contact the admin to get registered in the whitelist. There are a few drawbacks in the proposed system like the longer duration of registration than the normal login, On the mobile applications, it will need some changes.

(Bissada and Olmsted, 2017) mentions the use of three-factor authentication in mobiles as one factor i.e., username and password are already enforced. Another factor that they add is facial recognition with a combination of username and password. They used Microsoft Cognitive Services API instead of which a must secure version can be used. Also, the username and password authentication can be made stronger as they are stored in plain text only.

According to (Kumari *et al.*, 2017), In a contemporary data-driven culture, Big Data and Cloud of Things (CoT) are two intertwined research themes, and one study issue is to build an effective security solution that allows access to cloud-based resources, services, and data without jeopardizing the user's privacy. For implementation in a multi-cloud-server scenario, the author devised a biometrics-based authentication mechanism. The authors used bio-hashing to enhance the precision of biometric pattern matching. They then assess the scheme's effectiveness and efficiency to establish its value. It does not, however, include an identity update phase.

2.3 Others

(Huang *et al.*, 2011) talks about a method for the authentication of clients with the help of three distinct methods, namely: Passwords, Smart cards, and biometrics. Upgradation of two-factor authentication to three factors, a secure and generic framework had been proposed here. The solution proposed by them is quite good. However, biometrics may increase security, but error tolerance, privacy, and usability would be compromised. If a breach occurs in such types of systems not only the passwords of the users are compromised even biometrics like fingerprints can be easily stolen.

(Yu and Park, 2020) a lightweight three-factor authentication scheme with a secure user authentication system is proposed. Their system outperforms all previous state-of-the-art schemes in terms of efficiency and resilience against sensor node capture, replay attack, insider attack, and impersonation attack, as well as ensuring untraced ability and mutual authentication. However, Because of the large number of stored parameters in the smartcard, their approach is vulnerable to stolen smart cards and shared secret key guessing. Also, At the first communication session, there is no means to confirm the validity of the produced random number. In the event of a mobile phone or smart card being lost, a validation technique must be implemented to determine whether the user-generated the previously generated acceptable random number or not.

A three-factor authentication system based on facial recognition, gestures, and device ID, as well as a fuzzy matching engine, was introduced by SensiPass® as an IDaaS. (Stockdale *et al.*, 2015). Passwords are a common, if not ubiquitous, element of modern life. A username is used to recognize, and a password is used to authenticate a user in the traditional authentication approach. Both these aspects of the authentication procedure are textual in nature. Authentication mechanisms other than text have been proposed and, more recently, deployed. SensiPass® is one such approach with password less authentication solution.

3 Research Methodology

The research methodology had been adopted by looking at the current infrastructure of SensiPass® which is provided as an external authentication provider for clients. The research involved the use of the Microsoft Azure Active Directory. The purpose of this research was to integrate SensiPass® authentication three-factor digital dynamic signature with Microsoft Azure Active Directory's conditional access policy to create a disruptive IDaaS for Microsoft active directory.

3.1 Preliminary research

The preliminary research involved previous development conducted around multi-factor authentication and Identity and Access Management. The internship research project involved a three-factor digital dynamic signature authenticator around which the research has been conducted. The current SensiPass® method was studied, and the different modules and services were explored to understand the user workflow and process (Hill, Ruddy and SIROTA, 2012). The patent was carefully studied to grasp a good understanding of the methods and embodiments of the application. Multiple research articles, academic papers, and reports were also gathered from available sources such as IEEE to study the important details regarding the architecture, related applications, and implementation in order to support this methodology.

3.2 Analysis and research implementation

Threat analysis has been conducted by doing comprehensive research on various threats/Cyber-attacks and their linked NIST controlling family. A list of different types of attacks was drafted and put together in a tabular format with their description and overview.

During this phase of the research, various types of protocols came into the picture while conducting a comprehensive review like SAML and Open-Id. A comparison of various types of protocols has also been done to gain a good perspective of each one of them and choose the suitable one. Since the SensiPass® three-factor dynamic digital signature was combined with the Microsoft Azure active directory as an authenticator, various market leaders were also analyzed to gain an insight into the features, overview, and different services offered by them. The analysis of the different Cloud-based IAM service providers was performed to understand the different unique value propositions provided by each service provider and a gap study was performed to implement the research goal.

Conditional Access (CA) in Microsoft Azure Active Directory (AD) allows the user to create policies that analyse the Azure Active Directory access permissions requests to applications and give access once the request meets certain criteria. SensiPass®'s Three-factor dynamic digital signature (DDS3) provides a password less identity authentication system that is highly secure.

3.3 Pre-requisites

For conducting this research, we kept the following prerequisites in our mind:

- A premium active Azure AD subscription included conditional access where the P1/P2 licenses were assigned to each user that was logged in through SensiPass® MFA.
- An Azure admin service account was used to authorize access to the SensiPass® application. During the SensiPass® setup, this account requires the Azure Global Administrator role, but we can afterward decrease the service account's role privileges.

3.4 Evaluation of the research performed

Changes to the current Android application were proposed to comply with registration of an App on Azure AD and configuration on SensiPass® backends such as AppID, Public Key, and Secret Key. The final stage included the unit testing of each independent module and Integration testing of each module was performed to complete the end-to-end testing. The conclusion and future work were presented for possible feature addition and concluding the research work.

3.5 Research rationale

"SensiPass creates a sophisticated digital signature by empowering the user to create a secret interaction they can use to digitally modify their biometric signature, making it impossible for others to steal and imitate." – (Mike Hill, 2021)

A tremendous amount of organisational and regulatory pressure is created around businesses and firms to safeguard access to corporate resources. As a result, they can no longer safely allocate and monitor user credentials using manual and error-prone processes. IAM automates these processes while also allowing for extensive access control and auditing of all company assets, whether on-premises or in the cloud. To the best of our knowledge, various research has been conducted on multi-factor authentication systems, but human was always considered the weakest link in authentication when it comes to Identity and access management. The main motivation behind conducting this research was to address the problem of verifying credentials not human entities. During this research, an IDaaS solution has been applied to the Microsoft Azure Active Directory through the conditional access policy to create a new cloud-based authentication mechanism. Currently, no market leader is providing a three-factor dynamic digital signature authentication along with cloud integration which is an additional feature to help secure the clients their sensitive data. The current architecture has been built around cloud-only, client only, and for mixed architecture requirements. The architecture provides proximity to the end-user through which it is impossible for someone else to break the authentication process.

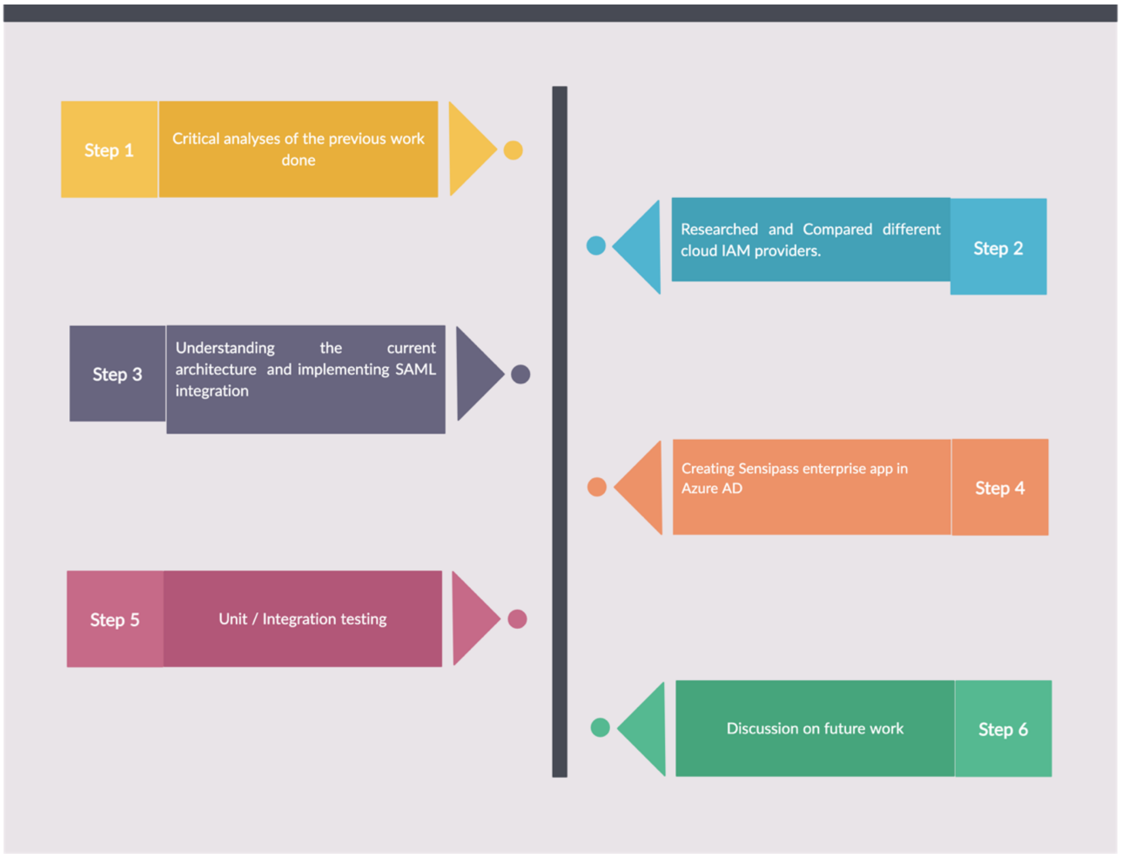

Step 1
Critical analyses of the previous work done
Researched and Compared different cloud IAM providers.
Step 2
Step 3
Understanding the current architecture and implementing SAML integration
Creating Sensipass enterprise app in Azure AD
Step 4
Step 5
Unit / Integration testing
Discussion on future work
Step 6

Figure 2. Steps for conducting the Research

4 Design Specification

Table 1 lists eighteen potential identity-related attacks caused by the IAM system's lack of security safeguards.

Table 1: Details of various attacks

Attack label	NIST 800-53 control family	Name of the attack	Attack description
A-1	SA-15(5)	API attacks	APIs that pose a danger to cloud IAM include reusable security tokens or passwords, as well as clear-text authentication. If left unprotected, cloud APIs are easily accessible over the internet, giving users high-level access to cloud resources.
A-2	SC- 4	Redirect URI manipulation	In a Redirect URI manipulation cyber-attack, an attacker targets the authentication request verification

			which is sent by the Identity Provider. To get access to the authorisation code started by the attacker, the target is sent to a website that is in control of the attacker. An attacker would then be able to access resources at the service provider by logging in as any user which is registered with the Identity Provider.
A-3	SC-23	Brute force attack	A brute force attack uses the hit and trial method to find out the login information, encryption keys, or locate a hidden web page. Attackers try all potential combinations in the hopes of making the right guess.[4]
A-4	AU-14	Snooping	Spoofing is when cybercriminals transmit messages to victims while posing as a trustworthy institution.[5]
A-5	AC12, AC-17, SC-23, AC-10, AU-14, SC10,	Session overwriting	The cybercriminal wants to force the user to use the malicious Discovery service provided by the criminal. The attacker makes the user's browser send 2 HTTP requests with the help of loading 2 HTML Iframes time shifted. Following the standard IODC protocol flow, the client identifies the malicious discovery service and erases the original metadata, and writes the new malicious metadata. The access token is received by the attacker and the access is granted to authorise resources from the service providers.
A-6	SC-23, SI-3(9), IA-2(8) (9)	Replay attacks	A replay attack is carried out when an attacker eavesdrops on a network communication that is secured. He then intercepts it,

[4] https://www.kaspersky.com/resource-center/definitions/brute-force-attack

[5] https://tweaklibrary.com/what-is-the-difference-between-spoofing-and-snooping/

			delays it, and then redirects the request to confuse the user into doing what the attacker wants.[6]
A-7	PE3(5), SA-18, SI-7(4), MP-5, SA19, SA-10	IDP confusion	The attacker alters data at user authentication endpoints, causing the service provider to deliver the access token to the malicious IDP incorrectly.
A-8	IA-12	Identity spoofing	In this type of attack, the identity of some other entity (human or non-human) is acquired by an attacker and then used in accomplishing a goal.[7]
A-9	AT-3, AT-2,	Phishing	Phishing is considered a social engineering attack in which a cybercriminal sends a fake message to a human entity who is a target in the hopes of acquiring sensitive information or deploying malicious software on the end user's infrastructure, like as ransomware.[8]
A-10	SA-10, MP-5, SA-18, SA19, SI-7(4), PE3(5)	Data tampering	When a malicious user intentionally alter (destroy, manipulat, or edit) data via some unauthorized channels is called data tampering.[9]
A-11	AU-10	Repudiation	A repudiation attack occurs when an application or system fails to provide controls to accurately track and log individuals' actions, allowing malicious manipulation or forgery of additional steps.[10]
A-12	SC-23	Eavesdropping	When a cybercriminal intercepts, deletes, or alters the data sent between two channels, it is known as an eavesdropping attack.
A-13	SC-23	Man in the Middle attack	In such a type of attack, an attacker secretly intercepts between two

[6] https://www.kaspersky.com/resource-center/definitions/replay-attack

[7] https://capec.mitre.org/data/definitions/151.html

[8] https://en.wikipedia.org/wiki/Phishing

[9] https://study.com/academy/lesson/what-is-data-tampering-definition-prevention.html

[10] https://owasp.org/www-community/attacks/Repudiation_Attack

			end-users who are communicating with each other directly.[11]
A-14	SA-4, SI-7, SA-3	Elevation of privilege	An insider with valid access raises their access privileges directly and gains unauthorized access, resulting in financial and data damage.
A-15	SC-5	Malicious endpoint attacks	Rather than targeting the servers, endpoint attacks target user systems. These contain four different types of attacks: (i) Service side request forgery (ii) Denial-of-service (iii) Code injections (iv) Broken end-user authentication.
A-16	SC-5	Denial of service attack	In a DoS attack, the attacker intends to shut down a network or system, blocking the users from accessing it. DoS attack is carried out by flooding the targeted machine or network with traffic or sending it such a piece of information that results in a crash.[12]
A-17	PA-4, PA-2	Identity propagation	The Facebook 2018 data breach showed that the users might expose their data to a service provider at the front end. However, The Service provider at the frontend may unknowingly or intentionally leak the PII to some other service provider at the backend with the user’s consent.
A-18	PA-2	User profiling	The metadata is exchanged whenever the SP (Service provider) contacts the IDP (Identity Provider). This includes information about the user's favourite websites, login attempts, and other actions. An honest SP may utilize the metadata details and

[11] https://internetofthingsagenda.techtarget.com/definition/man-in-the-middle-attack-MitM
[12] https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

			sell the information to third parties, jeopardizing user privacy.

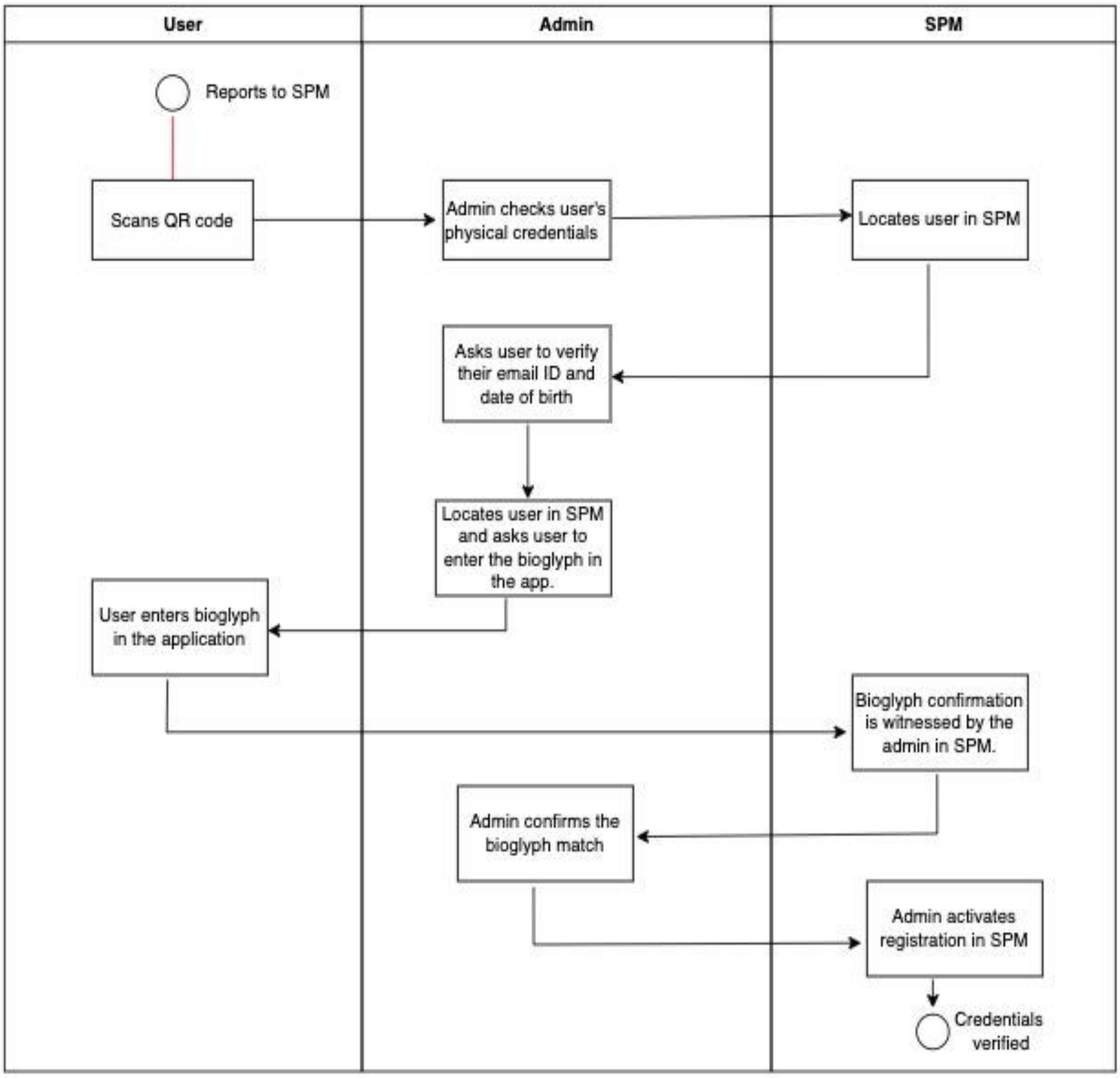

User
Admin
SPM
Reports to SPM
Scans QR code
Admin checks user's physical credentials
Locates user in SPM
Asks user to verify their email ID and date of birth
Locates user in SPM and asks user to enter the bioglyph in the app.
User enters bioglyph in the application
Bioglyph confirmation is witnessed by the admin in SPM.
Admin confirms the bioglyph match
Admin activates registration in SPM
Credentials verified

Figure 3. SensiPass® registration validation diagram

The flow diagram above depicts the registration and validation of the user's identity. When a user reports to the SensiPass Manager (SPM) admin, they scan a QR code after which the admin checks the physical credentials of the person, and then the user's credentials will be searched in the SPM. The user is then asked to verify the given credentials like DOB, email ID, etc. After that, the user is asked to enter the BioGlyph™ in the application. A BioGlyph™ is a selfie with a secret gesture (glyph) of the user's choice on it which is unique for every user. After entering the BioGlyph™, SPM confirms if it is matched or not. Admins confirm the match, and the registration is validated within the SPM for management within Azure AD.

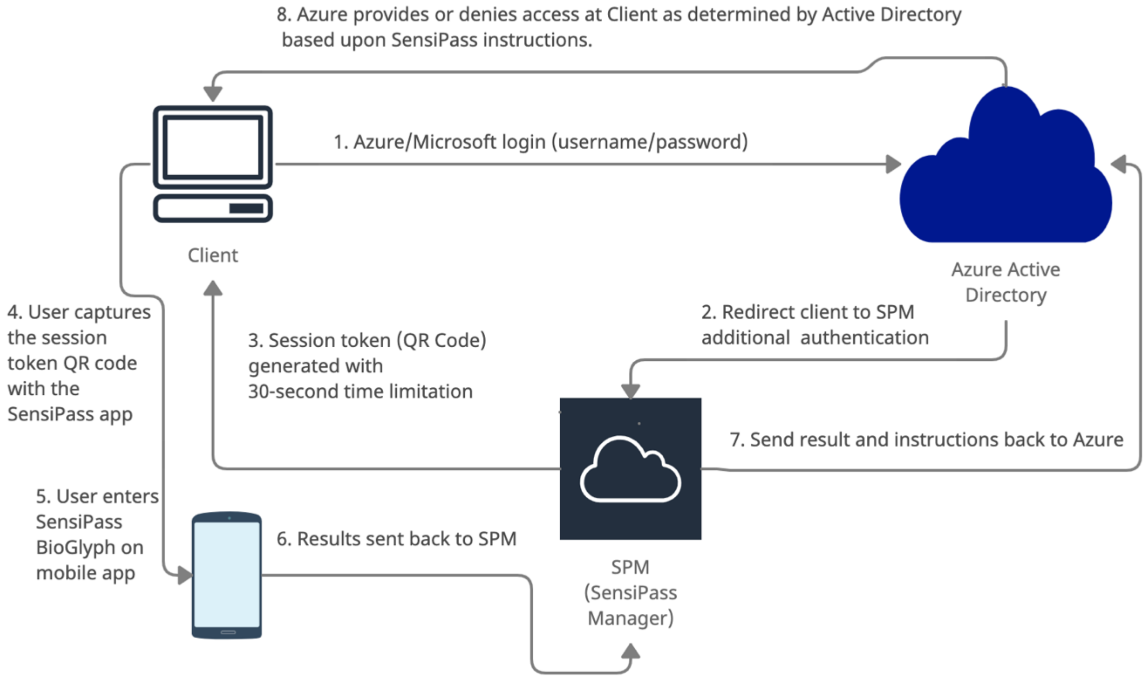

8. Azure provides or denies access at Client as determined by Active Directory based upon SensiPass instructions.
1. Azure/Microsoft login (username/password)
Client
Azure Active Directory
4. User captures the session token QR code with the SensiPass app
3. Session token (QR Code) generated with 30-second time limitation
2. Redirect client to SPM additional authentication
7. Send result and instructions back to Azure
5. User enters SensiPass BioGlyph on mobile app
6. Results sent back to SPM
SPM (SensiPass Manager)

Figure 4. SensiPass® Authentication Process with Azure AD Network

Figure 4 above shows the working of the architecture of SensiPass® combined with Azure AD. In step 1, the user logged in to Microsoft Azure Active Directory which further redirected the user's request to the SPM (SensiPass® Manager) for an additional authentication mechanism. A session token was generated (to confirm proximity to the Client) by SPM for 30 seconds for the user to scan. After scanning the QR code, the user was redirected to the SensiPass® mobile application authentication, user enters the BioGlyph™ after taking the selfie from the mobile phone. After the authentication is complete the results are sent back to the SPM further SPM forwards the result and instructions back to Azure. Based upon SensiPass instructions Azure provides access or denies it to the client. With the help of SensiPass®, the identities were managed and Azure was used to provide access management.

The Azure AD tenancy was simple to set up and was completely free too. Anyone who has a Microsoft account can easily set up their own tenant. Following the formation of the tenant, the application registration required a premium Azure AD membership. Premium P1 subscription prices $6 per user per month with a yearly agreement, and P2 subscription prices are $9. (Microsoft: Azure AD Pricing 2021). The P2 membership includes similar features as the P1 subscription. However, it also includes additional identity protection and management capabilities. Fortunately, it is possible to access premium services without a paid subscription even if it is a free tier user account.

Due to the lack of platform or methods to verify the usefulness of the higher assurance levels for authentication, several aspects of the research are based on theory and are speculative. Some parts of the research are theoretical and since it lacks an actual services subscription for testing the architecture for its effectiveness and requires enormous real-life environments and integration of proprietary IAM tools.

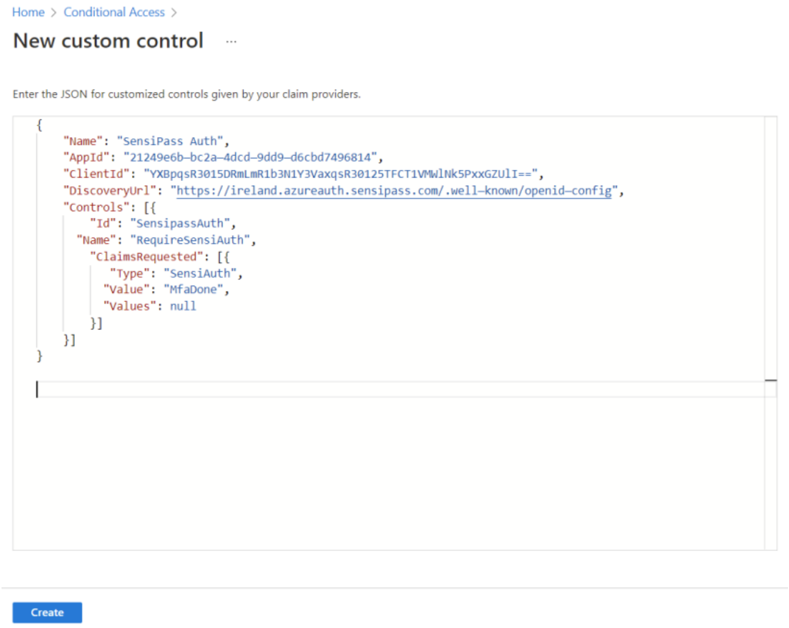
5 Implementation

Azure AD Conditional Access is used to create policies that analyse Azure Active Directory user access requests to apps and provide access only when the request meets certain criteria, such as user group membership, access device geolocation, or successful multifactor authentication.

SensiPass®'s Azure AD service adds an extra layer of security to Azure AD logins by having micro-level access policies and controls. It is used for providing the 3-factor authentication after the user enters the username and password for the application it wants to log in and gets redirected to a page where it can wait for SensiPass® application for authentication through its biometric and knowledge factor-based authentication.

Extending the current SensiPass® core services through SAML

Current SensiPass® architecture contained REST and SOAP API implementation for their existing core services. In order to trigger the push notification from Azure AD to SensiPass®, there was a need for an endpoint, that would wait for a POST request from Azure AD. The existing core needed an extension to build a SAML based Identity Provider. It also required a change in the existing android application which normally authenticates once it is opened by the user and the user does the authentication to complete the flow. In order to create a session-based push notification, a service was required to trigger the application once the user tries to login on Azure based apps that require the 3-Factor authentication when Azure AD conditional access conditions are met.



Enter the JSON for customized controls given by your claim providers.

```
{
    "Name": "SensiPass Auth",
    "AppId": "21249e6b-bc2a-4dcd-9dd9-d6cbd7496814",
    "ClientId": "YXBpqsR3015DRmLmR1b3N1Y3VaxqsR30125TFCT1VMWlNk5PxxGZUlI==",
    "DiscoveryUrl": "https://ireland.azureauth.sensipass.com/.well-known/openid-config",
    "Controls": [{
        "Id": "SensipassAuth",
      "Name": "RequireSensiAuth",
        "ClaimsRequested": [{
          "Type": "SensiAuth",
         "Value": "MfaDone",
         "Values": null
        }]
    }]
}
```

Figure 5. Custom Control Configuration in Azure AD Conditional Access

The custom control configuration shown in Figure 5 shows the JSON data that contains the configuration details for the SensiPass® Service endpoint. The DiscoveryUrl contains the SensiPass® service endpoint URL that will be triggered when a condition is met in Azure AD. Name, AppId, ClientId contain the details specific to the application and it should be unique for each Azure AD implementation. The "Controls" contains the ID and Name that will be sent to SensiPass® SAML based service and will be verified once the request is received. The ClaimsRequested contains the Type and Value for every request. There can be multiple values in ClaimsRequested based on different implementations, as it is an array based key.

6 Evaluation

This section of the report focuses on the evaluation of the implementation done in the earlier section. The evaluation had been done by comparing various protocols with SAML with different features and types of attacks. After which comparison of different identity providers had been done followed by a test case analysis of the changes implemented on the SensiPass current infrastructure.

6.1 Conducted a gap analysis based on the various security feature, mechanisms and protocols which are related to IAM.

Table 2 depicts that the mapping can also be used as a guide for cloud users to better understand the business's features and technological requirements, allowing them to make informed decisions when selecting suitable cloud IAM solutions. The findings from the mapping show that having the appropriate security features and mechanisms can avoid the identity threats outlined before (A-1 to A-18 in Table 1). Depending on the environment, IAM technologies and protocols also provide various security features, procedures, or contexts, but they may not meet all the security needs for a dynamically evolving cloud environment. However, a blend of methods and technologies will enable the creation of a successful IAM policy.

The reason behind choosing SAML for the integration is the diverse groups it targets. It enables the development and evolution of security systems and application software independent of each other. The reason behind it is that SAML provides a set of interoperable standard interfaces. A cheaper, faster, and reliable integration can be achieved by the standardisation of interfaces between the systems.[13]

[13] http://saml.xml.org/advantages-saml

Table 2: Mapping between various security features and mechanisms.

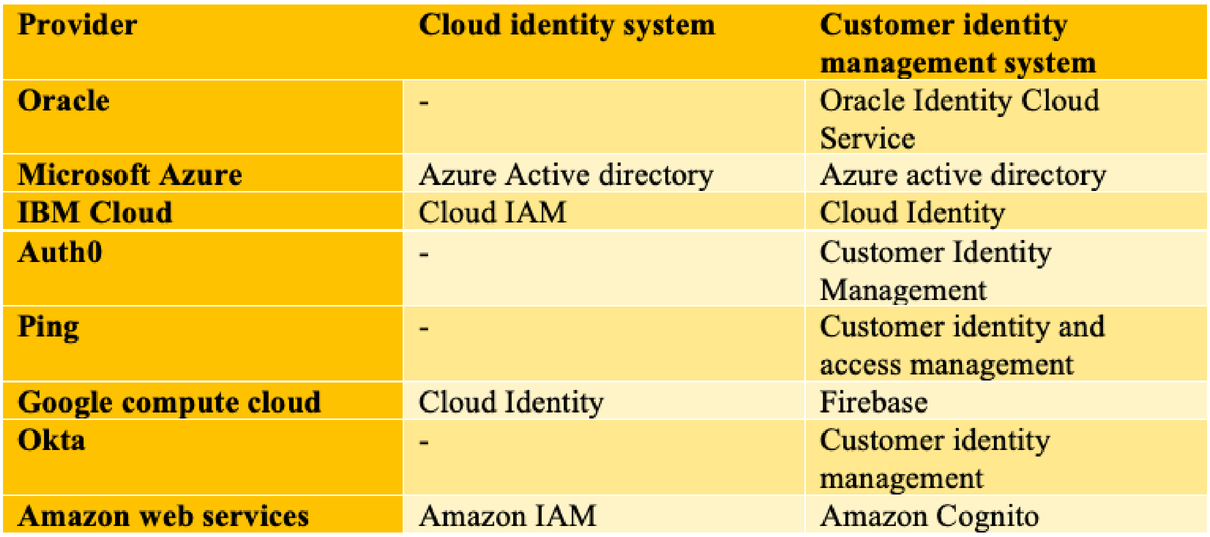
Features	Mechanism	Mitigated attacks	XACML	Open ID	SAML	0AUTH
Privacy	Usage of privacy standard	A-17, A-18	✗	✗		
	Remote administration of user policy	A-14		✗		
	Minimum disclosure	A-18, A-17, A-14, A-8		✓	✗	✓
	Use of Pseudonyms	A-18, A-17	✗	✓	✓	✓
	Anonymity	A-18, A-17		✗	✗	✗
Trustworthiness	Legal protection	-				
	Using open-source technologies	A-18, A-17	✓	✓		
	Segregation of duties	A-14	✓	✓		
Advanced features and capabilities	Reverse proxy capability	A-18, A-17, A-8, A-10	✗	✗	✗	✗
	Privilege access management	A-14, A-13, A-10, A-3	✗	✗	✗	✗
	Risk-based authentication	A-14, A-16, A-13, A-8, A-10, A-11, A-5, A-7, A-3	✗	✗	✗	✗
Security	Non-repudiation	A-11	✓	✓	✓	✓
	Encryption	A-18, A-17, A-8, A-	✓	✓	✓	✓

		12, A-10, A-4, A-9				
	Confidentiality	A-13, A-8, A-10	✓	✓	✓	✓
	Integrity	A-15, A-13, A-8, A-10	✓	✓	✓	✓
	Access control	A-15, A-4, A-8, A-18, A-10, A-3	✓	✓	✓	✓
	Authorization	A-14, A-6, A-8, A-12, A-10, A-9	✓	✓	✓	✓
	Authentication	A-14, A-16, A-6, A-8, A-12, A-11, A-9, A-3		✓	✓	✓
User-centric	Self-service	A-14		✗	✗	
	User Control and consent	A-14, A-10	✓	✓	✗	✓
User management, logging, auditing	Location independence	-		✓		
	Data Retention	A-11	✗	✗	✗	✗
	Digital Evidence	A-11		✗		
	Identity recovery	A-11		✗		

6.2 Analysed top cloud identity providers with the corresponding identity management services offered by them.

For managing cloud-based entities the next logical step is the adoption of IDaaS and cloud IAM solutions. IAM services are provided by cloud providers to manage the cloud administrators identities within the company, as well as they offer client IAM services to manage the identities of end-users, even if they are external customers or employees.

Table 3: Customer identity management system and cloud provider identification services



Provider	Cloud identity system	Customer identity management system
Oracle	-	Oracle Identity Cloud Service
Microsoft Azure	Azure Active directory	Azure active directory
IBM Cloud	Cloud IAM	Cloud Identity
Auth0	-	Customer Identity Management
Ping	-	Customer identity and access management
Google compute cloud	Cloud Identity	Firebase
Okta	-	Customer identity management
Amazon web services	Amazon IAM	Amazon Cognito

6.3 Test cases:

The table below depicts all the test cases depicted on the SensiPass side of the framework.

Table 4: Test case scenarios with actual results

Test Scenario	Actual Result	Module	Pass/Fail
User Authentication	User was successfully authenticated.	SensiPass®	Pass
User redirecting to SensiPass® page after Authenticating in Azure AD	User was redirected to the SensiPass® page after entering the username and password.	SensiPass®	Pass
Grant access check for SensiPass® Auth	The user was shown a notification on phone based on the control access enforcement	SensiPass®	Pass
API endpoints anonymous POST request check	The API was protected by API key and access denied was shown.	SensiPass®	Pass

6.4 Discussion

As per the evaluation done, the research shows a gap in the current multi-factor authentication framework where the authentication is performed with factors like username and passwords and neglecting the main important factor which is the human entity itself. A majority of multi-factor authentication providers consider the use of passwords, OTP safe whereas with the growing technology in the field of Artificial intelligence will soon prove the limits of these parameters. Verifying human entities rather than just credentials open a door to a new parameter in the domain of authentication. Following the completion of the data collection, a fresh set of criteria was established to develop the actual functional solution and to aid in the decision-making process. Identity theft is a major problem today, taking hold of a person's name, address, passwords, credit cards and more can create a great amount of chaos. Microsoft Azure is considered as a best-in-class IAM solution for the cloud, its integration with SensiPass® creates a very safe and secure environment for the client's usage.

7 Conclusion and Future Work

With the comprehensive evaluation, it can be concluded that adopting the integrated services of SensiPass® (identity management) and Microsoft Azure (Access management) can prove to be a real game changer in the domain of IDaaS. Passwords are disliked by most individuals, but malicious actors prefer them since they are common and easily abused. Despite these realities, legacy infrastructure limits, a lack of willingness to invest, and unwillingness to change have kept most enterprises relying on passwords for authentication. The trend to remote work has accelerated IAM transformation efforts and made employees more sensitive to change, which is a significant silver lining.

In the future, a blend of new technologies like artificial intelligence and blockchain will come into the forefront to safeguard identity management with the help of IDaaS providers like SensiPass® and its integration with other cloud computing service providers like AWS, Google Cloud and Oracle cloud.

References

[1] Kennedy, W. and Olmsted, A. (2017) 'Three factor authentication', in *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST). 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 212–213. doi:10.23919/ICITST.2017.8356384.

[2] Huang, X. *et al.* (2011) 'A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems', *IEEE Transactions on Parallel and Distributed Systems*, 22(8), pp. 1390–1397. doi:10.1109/TPDS.2010.206.

[3] ALSaleem, B.O. and Alshoshan, A.I. (2021) 'Multi-Factor Authentication to Systems Login', in *2021 National Computing Colleges Conference (NCCC). 2021 National Computing Colleges Conference (NCCC)*, pp. 1–4. doi:10.1109/NCCC49330.2021.9428806.

[4] Bissada, A. and Olmsted, A. (2017) 'Mobile multi-factor authentication', in *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST). 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 210–211. doi:10.23919/ICITST.2017.8356383.

[5] ALSaleem, B.O. and Alshoshan, A.I. (2021) 'Multi-Factor Authentication to Systems Login', in *2021 National Computing Colleges Conference (NCCC). 2021 National Computing Colleges Conference (NCCC)*, pp. 1–4. doi:10.1109/NCCC49330.2021.9428806.

[6] De Marsico, M. *et al.* (2014) 'FIRME: Face and Iris Recognition for Mobile Engagement', *Image and Vision Computing*, 32(12), pp. 1161–1172. doi:10.1016/j.imavis.2013.12.014.

[7] Li, C.-T. and Hwang, M.-S. (2010) 'An efficient biometrics-based remote user authentication scheme using smart cards', *Journal of Network and Computer Applications*, 33(1), pp. 1–5. doi:10.1016/j.jnca.2009.08.001

[8] Bhargav-Spantzel, A. *et al.* (2007) 'Privacy preserving multi-factor authentication with biometrics', *Journal of Computer Security*, 15(5), pp. 529–560. doi:10.3233/JCS-2007-15503.

[9] Goldwasser, S., Micali, S. and Rackoff, C. (1989) 'The Knowledge Complexity of Interactive Proof Systems', *SIAM Journal on Computing*, 18(1), pp. 186–208. doi:10.1137/0218012.

[10] Yu, S. and Park, Y. (2020) 'SLUA-WSN: Secure and Lightweight Three-Factor-Based User Authentication Protocol for Wireless Sensor Networks', *Sensors*, 20(15), p. 4143. doi:10.3390/s20154143.

[11]Kumari, S. *et al.* (2017) 'Design of a provably secure biometrics-based multi-cloud-server authentication scheme', *Future Generation Computer Systems*, 68, pp. 320–330. doi:10.1016/j.future.2016.10.004.

[12] Sharma, A., Sharma, S. and Dave, M. (2015) 'Identity and access management- a comprehensive study', in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT). 2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, pp. 1481–1485. doi:10.1109/ICGCIoT.2015.7380701.

[13] Tanwar, S., Tyagi, S. and Kumar, N. (2019) *Security and Privacy of Electronics Healthcare Records*,. doi:10.1049/PBHE020E.

[14] Stockdale, J. *et al.* (2015) 'A Fuzzy System for Three-Factor, Non-textual Authentication', in Arai, K., Kapoor, S., and Bhatia, R. (eds) *Intelligent Systems in Science and Information 2014*. Cham: Springer International Publishing (Studies in Computational Intelligence), pp. 125–137. doi:10.1007/978-3-319-14654-6_8.

[15] Hill, M.J., Ruddy, T.R. and SIROTA, R. (2012) 'Method and computer program for providing authentication to control access to a computer system'. Available at: https://patents.google.com/patent/WO2012164385A2/en (Accessed: 3 January 2022).

[16] Hughes, J. and Maler, E., 2005. Security assertion markup language (saml) v2. 0 technical overview. *OASIS SSTC Working Draft sstc-saml-tech-overview-2.0-draft-08, 13.*

[17] Saklikar, S. and Saha, S., 2007, November. Next steps for security assertion markup language (saml). In *Proceedings of the 2007 ACM workshop on Secure web services* (pp. 52-65).