International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V73I11P114

Volume 73 Issue 11, 173-192, November 2025

Review Article

Identity and Access Management (IAM) Federation, Tools, and Techniques: An Overview

Raja Viswanathan[1], Banumathi A[2], Manivel Kandasamy[3]

[1,2]*Research Department of Computer Science, Government Arts College (Autonomous), Karur, Affiliated to Bharathidasan University, Tiruchirappalli, Tamil Nadu, India.*
[1]*INFLIBNET Center, An IUC of UGC, Government of India, Gandhinagar, Gujarat, India.*
[3] *Department of Computer Science and Engineering, Unitedworld Institute of Technology, Karnavati University, Gandhinagar, Gujarat, India.*

[1]*Corresponding Author : rajamca66@gmail.com*

Received: 11 July 2025 Revised: 01 November 2025 Accepted: 10 November 2025 Published: 25 November 2025

Abstract - *Access and Identity Management (IAM) federations are an important area for protecting organizational resources and permitting seamless access across multiple domains. Still, modern IAM implementations are typically faced with challenges like inconsistent authentication schemes, fragmented access control, and cross-domain interoperability. These challenges highlight the gap in the research on securing, operationalizing, and the comfort level of IAM federation systems in hybrid and cloud environments. This paper will provide a fully-fledged discussion of IAM federation, including its tools, techniques, and applications in present-day organizations. The study of ten leading IAM tools and protocols, such as Single Sign-On (SSO), Multifactor Authentication (MFA), Privileged Access Management (PAM), SAML, OAuth, and OpenID Connect, will comprise a part of the research undertaken on a qualitative comparative review methodology. They are evaluated based on the strength of security, interoperability, compliance with regulations (GDPR, HIPAA, FERPA), and usability. The results show that SAML and OAuth protocols give better assurance of security, while SSO and PAM are better in usability and governance efficiencies. The paper is helpful because it provides a simple model of federated IAM definition, illustrating both the technical advantages and drawbacks that are present today. It also argues about the ethical and data compliance implications, indicating where the future enterprise system federation models of AI should be developed.*

Keywords - *Identity and Access Management (IAM), IAM Federation, Security Protocols, Single Sign-On (SSO), Multifactor Authentication (MFA)***.**

1. Introduction

In an era of digital interconnectivity, secure and effective systems for user identity and access to resources in organizations must exist. Identity and Access Management (IAM) is all of the policies, technology, and processes that ensure individuals are entitled to access designated resources for a legitimate purpose and at an appropriate time [1]. Components of IAM include, but are not limited to, authentication, authorization, user lifecycle management, and regulatory compliance. Federation in IAM refers to the application of those principles, including authentication and authorization, to multiple organizations or domains, allowing users to access resources in other systems with only one trusted authentication method [2].Companies are transitioning to hybrid cloud and multi-domain ecosystems as they continue to push forward digital transformation initiatives [9]. While this is the case, virtually all existing deployments of Identity and Access Management (IAM) systems are siloed in nature and provide little to no value or support for interoperability across systems [3]. Therefore, several issues have emerged, including redundant identity stores, conflicting authentication policies, and greater vulnerability to data breaches [12]. Previous studies have evaluated specific IAM implementations such as Single Sign-On (SSO) and Multifactor Authentication (MFA); however, an overall comparative assessment of federated IAM implementations, given the current state of scale, data compliance, and cross-domain operability, is lacking [10]. The lack of research points to the need for a unified investigation of a federated IAM implementation and how it would improve security and experience for the end user (identity).This paper is unparalleled in that it provides a comprehensive analysis of the federated IAM protocols and tools, such as Security Assertion Markup Language (SAML), OAuth, OpenID Connect (OIDC), Privileged Access Management (PAM), and others. In the paper, these technologies are evaluated in a distinctive approach that evaluates their interoperability, compliance with data protection law, and security

performance [4]. This research integrates contemporary literature and technology, and provides a systematic understanding of the role IAM federation plays in enhancing security posture in organizations, enabling control of identity management, and supporting compliance with rules and regulations in multi-organizational environments [11].

These are the main goals of the proposed study:

- This article will introduce the IAM Federation by discussing this framework's idea, advantages, and use in streamlining authentication and authorization for users across many domains.
- To assess the protocols and tools for IAM federation: Evaluate OpenID Connect, OAuth, SAML, and other technologies and protocols used in identity and access management federation.
- To examine IAM Federation Methods: Investigate the several methods for setting up federated identity connections, including trust frameworks, federation servers, and identity brokers.
- When evaluating Security Considerations, examine the possible risks of cross-domain access, SSO, and other security issues with the IAM federation and provide solutions to these problems.
- To examine Regulatory Compliance: Within multi-organization settings, analyze the function of IAM federation in ensuring adherence to data protection regulations like GDPR, HIPAA, and FERPA.

1.1. Contribution

This paper discusses an overview of the identity and access management federation. First, it shows how the IAM federation will work in different organizational environments. Secondly, it explores that many tools and techniques are used in IAM to control and manage access for authorized accounts and applications. This paper also explains the related works and finds how IAM worked in various roles in different organizations. SSO, MFA, PAM, SAML, OAuth, OpenID Connect, etc., are some critical IAM tools and techniques that are mainly focused on in this study [20]. The article provides a solution to single sign-on and cross-domain access risks. This work includes information about common trust frameworks in the IAM federation, such as SAML, OpenID Connect, OAuth, etc [6].

2. Literature Review

Identity and Access Management (IAM) is a dynamic subject that is at the heart of providing secure digital access both inside and outside the organization [5]. The history of IAM has been that of evolution as basic credential-based systems have evolved into all-encompassing models that incorporate authentication, authorization, compliance, and lifecycle management. In a federation environment, IAM facilitates the establishment of trust between a number of organizations so that users can be authenticated in one place and be able to access a number of systems without any security threats [15]. The literature has shown an increasing role of IAM federations in facilitating digital transformation, hybrid cloud, and cross-domain interoperability.

Initial researches on IAM were centered on centralized authorization and authentication. These systems were effective in a single organization, but in most cases, they lacked scalability and cross-domain interoperability when applied to other areas [7]. Other research also suggested federated IAM designs that allowed identity data sharing securely via standards like SAML, OAuth, and OpenID Connect [21]. These frameworks were more adaptable, but organizations encountered many challenges of compliance, policy management, and real-time threat detection [6].

The most recent innovations from 2023 to 2025 have dramatically expanded IAM capabilities due to the incorporation of Zero Trust principles and AI. Zero-trust-based IAM architectures have replaced perimeter-based models of security by rebuilding verifications at all potential access points [16]. These frameworks also allow dynamic access controls, live policy controls, and enhanced resistance to identity-based attacks [27]. Studies have shown that IAM in zero trust architecture enhanced identity assurance by more than 30 percent, reduced credential theft, and improved auditability of distributed systems [24]. These represent the paradigm shift of traditional access control to context-aware dynamic authentication [25].

Similarly, AI-powered IAM systems have become an effective tool to handle intricate and large-scale identity environments. Login patterns, anomaly detection, and automating access provisioning are now being undertaken using machine learning algorithms and behavioral analytics [26, 30]. IAM solutions based on AI can detect unusual behavior, neutralize the threat of insiders, and decrease the number of administrative activities through the automation of identity governance operations. They can also enhance the accuracy of authentication and increase compliance by dynamically enforcing policy rules. The intersection of IAM and AI means that the identity management systems will be changed significantly in terms of self-learning, predictive, and risk-sensitive [28].

The other significant subject in literature is the regulation and data governance in the IAM federations. With the exchange of identity information between the organizations and between the platforms, it is necessary to guarantee that the organizations comply with data protection laws, including GDPR, HIPAA, and FERPA. Current IAM applications are aligned to the application, with compliance-related features regarding implemented audit trails with security standards, encryption specifications, and access control mechanisms [33]. Scholars have also noted that federated IAM systems

make it easy to manage authentication, yet some of the benefits are accountability and transparency in data management from an enterprise perspective [14]. A compliance-based design would align the identity management processes with organizational policies, and, where applicable, with laws at the international level [21].Concerns have also been raised regarding cloud-based IAM in the recent past. As enterprises transition towards hybrid and multi-cloud approaches, federation in identity management denotes that the federated identity will have consistent security policies across all systems [13].

Research demonstrates that the use of IAM federations in cloud environments will enhance interactions among different service offerings, such as SaaS, PaaS, and IaaS, while reducing administration processes and providing consistent user permissions across each offering [18]. However, there have been concerns about the overall integration among systems and the ideal balance between enhancing usability and ensuring security measures are implemented.Even recent developments in research highlight, at the same time, the ethics and privacy implications of federated IAM systems. With the rise of shared identity services, privacy-preserving, and data minimization, strategic authentication has become so important [23]. Various proposals for encryption, pseudonymization, and anonymization have been developed to protect sensitive identity data while maintaining usability and compliance [29]. Furthermore, continuous surveillance and sophisticated identity governance in the federated ecosystem are considered critical stages toward reducing illegitimate access and data breaches [34]. Overall, the literature suggests that IAM is on a distinct trajectory and evolution, and IAM systems today are progressing to intelligent, federated, and compliance systems. Also, Zero Trust, AI-driven automation, and compliance regulation are arguably part of the current state of the art in identity management. Nevertheless, there are still loopholes in ensuring that IAM standards interoperate with each other and in the creation of coherent frameworks that can easily interconnect security, compliance, and user experience. Information on how to overcome these limitations will offer a solid basis for the way IAM federation will proceed to be more resilient and ethical in operations and governance.

3. Research Methodology

Figure 1 displays the Conceptual Framework of IAM Federation Evaluation that will show the way the given study is organized. It includes four layers: the Input Layer that relies on the literature and frameworks like SAML, OAuth, OIDC, and GDPR; the Evaluation Criteria layer, which outlines such parameters as security, scalability, interoperability, and compliance; the IAM Federation Tools layer, which includes such technologies as SSO, MFA, PAM, SAML, OAuth, and OpenID Connect; and the Output Layer which provides a summary of the comparative results, which are best practices, performance gaps, and key findings.

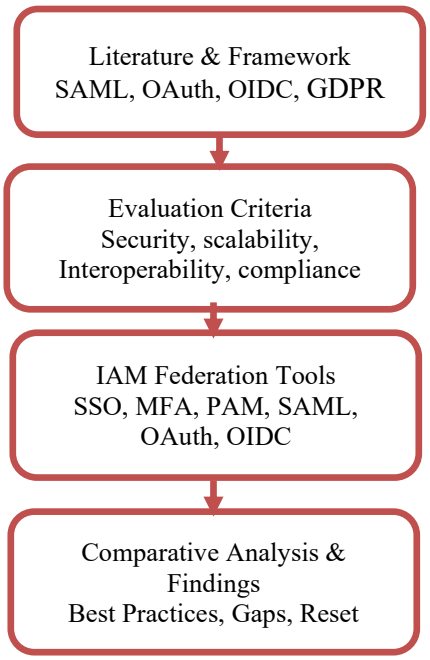

Fig. 1 Conceptual framework of IAM federation evaluation

The framework provides a good top-down view of how IAM federation tools were researched and investigated.

3.1. Research Approach

The research is framed in a qualitative and comparative research methodology to explore the tools and techniques that can be implemented in an IAM federation. The evaluation aims to understand how different IAM frameworks facilitate authentication, authorization, and compliance within a federated environment. The research is a model review and analysis of secondary data to investigate the strengths and weaknesses of the selected IAM tools, as well as the potential for integration.

3.2. Data Set

The article is based on secondary data collected from academic journals, technical reports, framework documentation, and compliance guidelines. Among the important materials are standard recommendations, which include SAML, OAuth, and OpenID Connect, as well as identity and access management guidelines from significant providers such as Azure, AWS, and Okta. The compliance features were also examined through relevant governing compliance frameworks, including GDPR, HIPAA, and FERPA.

3.3. Evaluation Criteria

All IAM tools and protocols were evaluated based on five criteria: security, scalability, interoperability, preparation for compliance, and user experience. These criteria are used to evaluate the suitability of each framework with regard to identity management, data protection, and cross-domain consistency in federated systems.

3.4. Tools Reviewed

The text outlines six distinct cybersecurity measures, including Single Sign-On (SSO) methodology, Multifactor Authentication (MFA) safeguarding technique, Privilege Access Administration (PAM) regulatory framework, Security Assertions Markup Language (SAML), OAuth standardization process, and OpenID Connect identity verification scheme [17]. Among these options, they were chosen because of their widespread use and relevance in both enterprise-level and cloud-based identity management solutions [22]. Their analysis was conducted according to authentication methods, integration capacities, and preparedness for regulations.

3.5. Analytical Overview

A focused analysis was conducted to define each mechanism's performance based on each of the selected criteria. The comparison demonstrated that SAML, OAuth, and OpenID Connect are more interoperable and more readily prepared for compliance, in contrast to MFA and PAM, which are efficient security mechanisms. The findings have been used to suggest reasoning to make a more cohesive view of the role of IAM federation to improve security, aid in streamlining access control and management mechanisms for the protection of data in multi-organization contexts.

4. Role of IAM Federation in Multi-Organization Environments

IAM plays vital roles in multi-organization environments, such as identity and access management functions in improving cyber security awareness, IAM applications in hybrid cloud environments, and the IAM integration with zero-trust security structures. Implementing the IAM system is essential to improving cybersecurity awareness in all organizations. Organizations should develop proper protocols and rules for user authentication and access control by introducing IAM solutions, because it is significant for educating staff about security practices. IAM supports protecting confidential credentials and allows workers to actively protect the organization's digital resources by developing an accountability culture where users can recognize their responsibilities and rights concerning access.

The zero-trust model's key tenets, by IAM integration, were "never trust, always verify". It requires continuing authentication of user identities and permissions, besides their area in dealings with the organization's network system. Implementing IAM was vital for controlling identities and access through varied platforms, especially as organizations highly approve of hybrid cloud environments. IAM solution permits organizations to integrate identity governance through a devised environment, confirming reliable enforcement of access policies and even managing user identities [25]. IAM solutions identified the new solution to the security problems through many workers linked to the corporate center from various places and devices. It confirms remote access safety in a highly robust manner by implementing adaptive authentication patterns from multiple relevant elements, including device, location, and usage habits. IAM plays an integral part in safeguarding against insider threats. Insider threats, such as contractors, workers, and other agents, are hazardous to enterprise security. IAM federation supports those block-like openings by strong access controls observing the least privilege principle, and it allows workers to access only data when related to their task. The IAM Federation guarantees adherence to data privacy laws through its involvement in identity management processes. The IAM federation facilitates verifying adherence to data privacy laws, such as FERPA, GDPR, and HIPAA, through unified identity administration, transparent logs of activities, and precise permission settings [27].

The IAM solution has encountered numerous privacy hazards related to data storage, collection, and management of user identities. Many identity management federation systems necessitate additional sensitive data for authentication purposes. Adhering to laws like GDPR, CCPA, HIPAA, and FERPA ensures compliance due to their mandates for safeguarding personal info and monitoring usage practices. IAM federation helps with specific regulations like GDPR by data minimization and Data Subject Access Requests (DSARs) [26]. IAM federation simplifies the authentication and control of critical data related to separate users, who permit efficient responses to DSARs. Data minimization is supported by applying granular access controls depending on user characteristics, and IAM will certify that only the official user gets permission to access essential data. The IAM federation supports Protected Health Information (PHI) and compliance reporting in HIPAA. IAM federation provides substantial access control to PHI because it only allows strong access controls against unauthorized usage. It will certify that only authorized healthcare users can use patient credentials. Complete audit trails inside the IAM system will permit healthcare associations to establish devotion to HIPAA data privacy needs [29]. For FERPA, IAM will support parental access controls and student data protection. IAM federations set access to student qualifications reports depending on their roles, such as administrators and teachers, to confirm their data privacy. IAM federations are essential in preserving data protection compliance by offering centralized devices for controlling individual user identities. It also applies granular access controls and handles complete audit trails. It also makes things simple for important components for organizations in managing critical data under regulatory compliance, such as FERPA, HIPAA, and GDPR. Within an Identity and Access Management (IAM) framework, the federated entity manages interactions between Identity Providers (IDPs), which authenticate users, and Service Providers (SPs), which grant access rights based on these authentications. A credential-based authentication service enables authenticated individuals to gain entry into various software programs via their unique identifiers. A third-party entity acts as a bridge connecting an

authentication authority to a service vendor. Additionally, it specifies how users identify themselves and determines varying degrees of system access according to the trust agreements made between them. In the IAM federation, the federation server is responsible for creating the protocols and rules for user authentication in various applications. Generally, federation servers do not directly work in user authentication, but they confirm whether the procedure is safe.

In a standardized federation, the identity brokers support business value to the Relying Parties (the RPs) and Identity Providers (IdPs). RPs and IdPs are only required to integrate with the identity broker once. The RP value is easy once it connects with the identity broker and obtains many categories of credentials. An identity broker regulates the proper access for users depending on their application and identity, where they wish to access. When evaluating IAM's security considerations, Single sign-on and cross-domain access have some problems in implementation [22]. Generally, implementing SSO and cross-domain access has several key possible dangers, such as leading to a single point of failure, an elevated attack surface, credential theft, and improper session management. It is also dangerous when they always depend on third-party providers, as this can lead to cross-domain vulnerabilities and privacy concerns. These are the key dangers of single sign-on and cross-domain access in the IAM federation. The main problem among these is the single point of failure. If the single sign-on system is compromised or even experiences an outage, the User will lose all the access linked to applications. It will cause severe trouble for operations. When unauthorized users get access from a specific user, they can access all applications associated with that User [6]. Strong authentication methods and regular security audits are better solutions to overcome this problem, which occurs in cross-domain access and SSO.

Implementing multifactor authentication will help users add extra protection when logging in to the SSO application. If hackers get one credential from users, they need to get more access, so it is difficult for them to access other users' accounts. Then, organizations should frequently monitor user actions in their applications because it will alert users when another unauthorized user tries to access their applications.

4.1. Tools and Techniques of Identity and Access Management

4.1.1. Single Sign-On (SSO)

Single Sign-On is a key tool used in identity and access management. SSO allows users to log in to numerous applications with a single login. This tool makes it simple to manage multiple passwords and accounts. It creates authentication for a user, including access permissions and user credentials, and allows the User to access all allowable applications. After allowing access to one application, all other applications permit that User. To access the authenticated one application. This verification is reusable for other legalized applications without getting a username and password [6]. The purpose of using SSO is to improve security and communication during user verification and access permission confirmation, and it also helps in the reduction of management costs. Accessibility, implementation, functionality, confidentiality, expandability, interoperability, integrity, and upkeep define single sign-on features. The Single Sign-On system relies on an Identity Provider for authentication, followed by a Service Provider's validation of credentials via Assertions. A directory service houses authentication credentials for users. An entity responsible for providing Services (S), which requires user verification when accessed through an interface. The assertion represents the data conveyed by the Identity Provider (IdP) to the Service Provider (SP).

Table 1. MFA approaches, advantages, and disadvantages

MFA Methods	Advantages	Disadvantages	Applications
Biometric	Highly secure, Unique physical traits, complex to take off	Raises privacy concerns, cannot reset	Healthcare and finance
Smart card	link knowledge-based and physical security	Need a card reader and a comfortable chair	Banking and government.
Passwordless	Decrease password risk, increase convenience	Trusts in secure device management	Technology and banking

According to Figure 2, users can initiate an inquiry by requesting access to a separate online site via the intermediary service provided through their internet browsing tool. When users are not authenticated, the system directs them to an authentication server via their internet-connected device's default web interface. Subsequently, verification of the user's data takes place, followed by their redirection to an authentication service. Subsequently, the individual encounters a login screen where they input their identifying information for access purposes. When the authentication process verifies the user's credentials, it triggers the service provider to redirect the user to the reverse proxy along with their identifying data. RP will obtain the persistent identifiers information from the REMOTE-User setting variable and chart the user credentials for third-party websites in the reverse proxy database. Reverse proxy automatically logs on the User's behalf depending on the extracted user identification information. The 3PW web content is sent to the User when the User is authenticated. The main advantage of using SSO is that availability will be high, and integrity will decrease as it depends on the security solutions. Implementing single sign-on technology can help users improve productivity

by not having them validate every application separately. It is easy to adapt SSO for new applications or new software programming. Using the SSO feature, organizations expect high safety to build faith in their clients. They are safely enabling users and introducing diverse user authentication, such as biometrics and passwords [7]. They also used hardware tokens such as certificates, smart cards, digital signatures, and network standards such as SAML and Kerberos [31]. The major disadvantage is that applying SSO in the company may provide intruders a chance to reach all servers and applications in the network. Whenever the company resolves to use Single Sign-On, it has to face the main challenges of combining numerous systems, especially in security and architecture. When establishing, implementing, and maintaining Single Sign-On, the organization faces infrastructure, security, and user access challenges. In infrastructure, during execution, it is extended beyond what is expected to set up SSO.

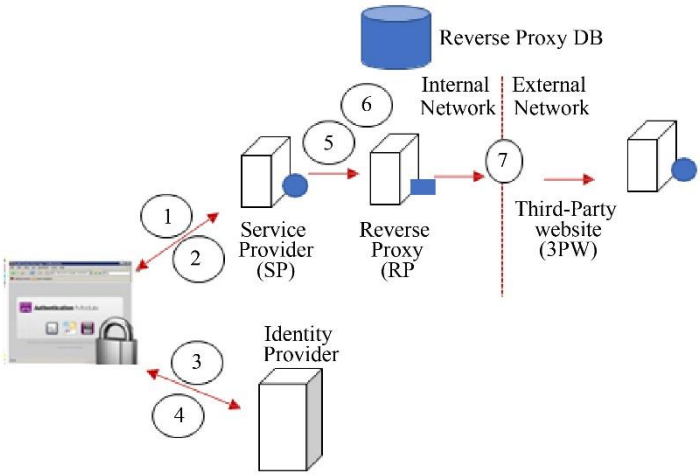

Fig. 2 Single sign-on architecture

4.1.2. Multifactor Authentication (MFA)

The multifactor authentication function enhances security by requiring multiple forms of verification for accessing online assets. Users must input additional information beyond their login credentials to access application features. Enhancing security further through this approach involves requiring additional authentication methods such as biometric scans, SMS codes delivered to mobile devices, or physical access keys. The term "multi-factor" is derived because it incorporates multiple forms of verification. There are typically four primary types of authentication techniques categorized as follows: those based on knowledge ("what you know") such as passwords or PINs; physical possessions ("what you possess"), exemplified by cards or tokens; biometrics ("who you are"), including features like fingerprints or speech analysis; and behavioral patterns ("how you act").

Among various methods, such as biometrics, smart cards paired with PINs, and non-password-based systems, these three stand out as leading options for enabling multi-factor verification due to their emphasis on enhancing security in critical situations. Multi-factor authentication plays a crucial role in safeguarding cloud services, IoT systems, vital networks, and secure online connections. Several prominent cloud service providers, such as Microsoft Azure, Google Cloud Platform, and AWS, integrate multi-factor authentication into their safeguarding mechanisms to ensure secure access for legitimate clients exclusively. In remote access security, MFA addresses the risk of unsecured networks by certifying that access to complex company resources is allowed only after verifying numerous authentication steps [10]. Table 1 includes the methods of MFA and their advantages, disadvantages, and applications. Biometric, smart card, and passwordless are three methods of MFA. Biometrics have high security and are highly used in healthcare and finance applications [8]. The smart card has physical security, but it is less convenient. Passwordless has reduced the danger of passwords and is highly used in banking and other technologies.

Figure 3 displays a dataflow diagram of multifactor authentication. Firstly, the client side loads fingerprint images into the system using an interface operator. The features are encoded and sent to the server. When these features are reached at a server in encoded form, the server has that and sends One Time Passwords (OTP) from the OTP generator. OTP generator is generally considered a function set on the server machine. The time-coordinated OTP is sent to the authorized phone number. Then, the User's mobile phone automatically receives OTP, which is likened to server-made OTP on the server side [11]. If OTP is confirmed, the server will request the User’s iris. The server confirms the iris image through a network that stores the iris pattern in its database. Getting original data so quickly is impossible is impossible is impossible because the iris image is already stored in the encrypted pattern. So, even if an intruder gets hash codes through the database, verification can be positive.

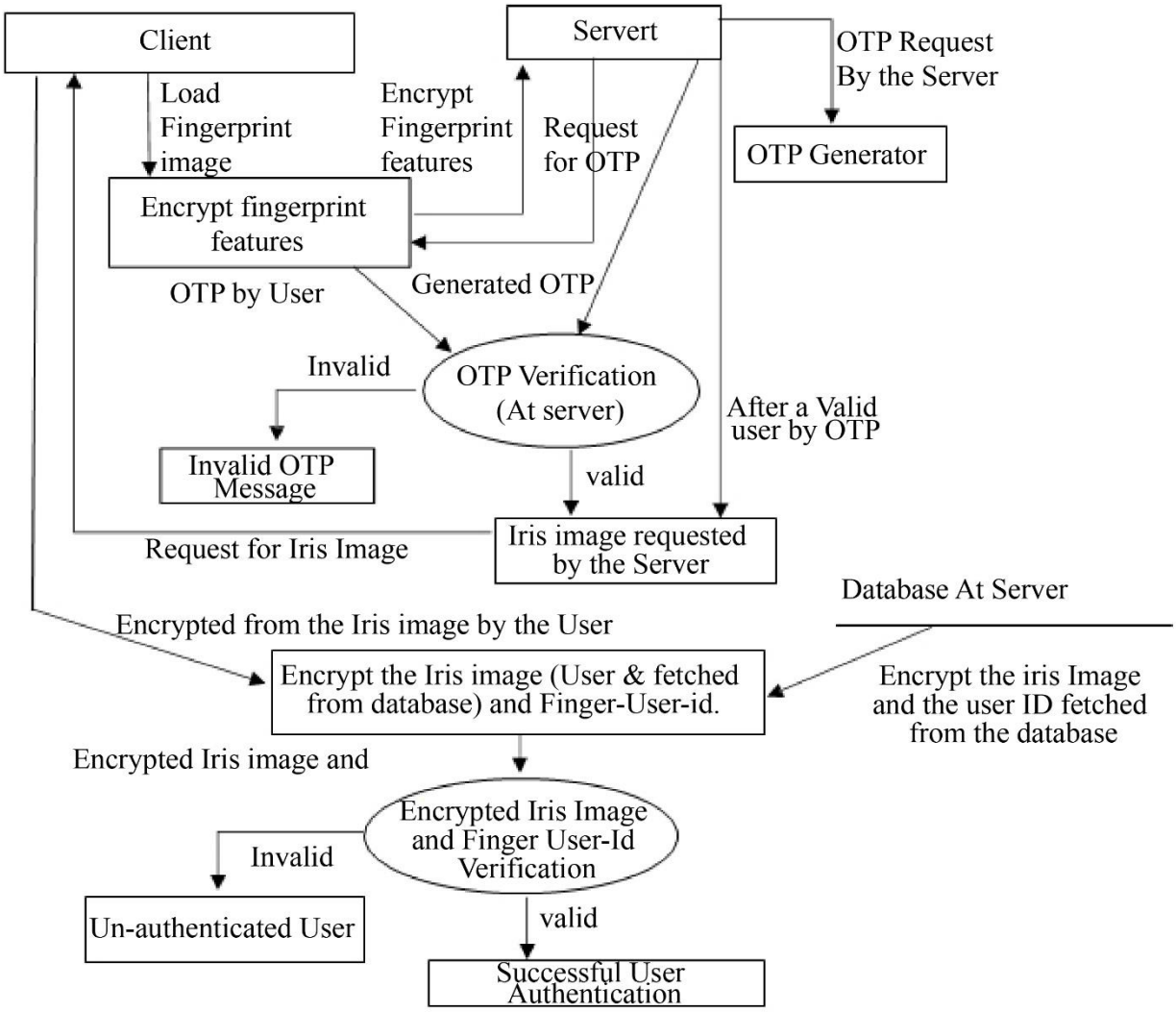

Fig. 3 Dataflow diagram of MFA

If both the fingerprint hash code and the iris image are matched, the User is verified as an authorized user. In short, the authentication is only successful when the fingerprint hash code, OTP, and iris images are matched. If someone's iris images or fingerprint hash code has no matches, then the User is recognized as unauthorized. If OTP has no matches, then the User is blocked by the authentication process. There are numerous benefits to multifactor authentication in terms of identity and access management. The most important benefit is securing identity and access management. Because MFA requires users to provide more than one form of verification, like passwords, it is even more difficult for hackers to breach their accounts. MFA significantly reduces the risk associated with using weak passwords. There is also a high degree of flexibility with the authentication methods, and there are fewer risks of identity theft. The principal downside to MFA is that it has added difficulty to the login process. It involves users having to recall and interact with multiple forms of authentication verification, which can be frustrating and require excessive amounts of time. Applying MFA may require some cost because of buying hardware tokens, training staff on new security protocols, and software licenses. It often trusts external aspects like internet connectivity to obtain authentication codes. This support may be delayed in areas with weak connections. Multifactor authentication has high challenges in usability, security, integration, privacy, probabilistic behavior, and robustness [13]. User inconvenience is common in MFA because of extra verification steps.

4.1.3. Privileged Access Management

Privileged Access Management (PAM) is the cybersecurity strategy that guards essential data and systems from unauthorized users. It uses a combination of persons, procedures, and technology to observe and control privileged accounts. Nowadays, organizations are handling many cybersecurity challenges and legal disturbances that users pose. Privileged Access Management will assist in difficult

times and is recognized as a security support for controlling illegal activity and accessing data [15]. PAM shows the complete technology, rules, and operations mainly designed to protect authorized accounts. PAM plays an essential role in access management. PAM also supports organizations in defending their significant assets and decreasing the danger of data breaches. PAM works through authentication, authorization, and auditing.

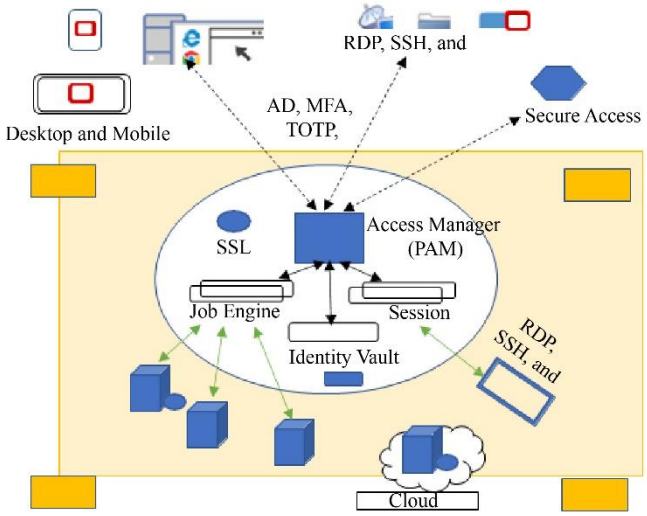

Fig. 4 Working architecture of PAM

Figure 4 shows the working architecture of PAM. PAM servers can be connected to single or multiple virtual computers. All computers should be recognized as nodes. A single-node system is generally straightforward and fast. However, many organizations will plan to use multiple nodes for the server connection to improve convenience, develop performance, and provide high security. The job engine is the blthathat executes background processes, such as creating or resetting words. Accumulating many job engines improves the speed of tasks because all of them are performed simultaneously. The session manager is basically the jump server gateway. It shows distant computer screens in the User's browser. The server may include many session managers. Each session manager should manage frequent sessions. RDBMS is one of the blocks that help supply all internal system data. [15]. The server will cover only one RDBMS node. The server is equipped with an internal database connected to one of the nodes, which contains a job engine or Application GUI. People should install a privileged access management node in an isolated network to offer access to resources in the isolated network. One node in the network will assist all resources it can use within this network. The isolated node will connect via its internal database and then be arranged to serve as an isolated node. It does not want to link to the same database because the core PAM node is connected in this deployment scenario, which means that the back-end database of the key PAM node is not available to the isolated node from within its network. After that, the session manager helps to offer isolated access to a particular network, and then the node desires to connect to the session manager for a remote network through the PAM proprietary protocol.

The session manager traffic among the isolated nodes and the central node is protected by certificates swapped between the nodes. PAM has a great advantage in the IAM federation because it can improve security by managing access to authorized applications. It also develops visibility into privileged user action, improves compliance with regulations, and qualifies inside threats. PAM severely controls privileged accounts, so it lessens unauthorized access and cyberattacks. PAM has high operational efficiency and automatic password management [16]. PAM also has disadvantages, such as the complexity of implementing PAM. Because it needs careful scheduling, it is combined with the existing IT infrastructure and operator training. Another advantage is that it will be high cost because, based on the size and complexity of the organization, the robust PAM cost will be significant, including maintenance and licensing fees. Executing privileged access management significantly decreases the risk of cyber-attacks and improves compliance. Organizations will face many issues in complexity, compliance requirements, scalability, integration with legacy systems, and security risks. It has problems such as hard-coded credentials, decentralized credential management, and forgotten accounts.

4.2. Security Assertion Markup Language (SAML)

The Security Assertion Markup Language (SAML) stands as the predominant method for establishing identity verification across organizational boundaries. This universal login system enables access across multiple programs through a shared credential. This system utilizes XML to ensure compatibility among providers of services and those managing identities. SAML works will depend on the response or request of the service provider. One side requests specific individuality data, and the other side's identity provider replies with the data so that the User can be verified and authenticated in the end. It provides many benefits, such as: it improves security by integrating authentication and developing a user experience with the single sign-on. It also helps streamline identity management and improve compatibility with various applications due to its open standard nature [17]. SAML can support organizations by reducing their administrative burden. It has a high advantage in decreasing password fatigue. It can develop complete security by trusting a dedicated identity provider to handle user identifications. Even though it has several benefits, its key disadvantage is that it does not permit a federation to form dynamically to allow service provisioning in real-time. SAML has challenges in implementing and has struggled with troubleshooting because of its verbose nature. It has a debugging difficulty that troubleshooting a problem with SAML will be difficult because of its intricate connection between SPs and IdPs when dealing with several providers. Figure 5 presents an illustration of the Single Authentication

Message-Layer protocol for user identity verification. An intermediary organization works in conjunction with another entity to create a secure means for exchanging information efficiently between them. To establish communication with their designated host, this cloud solution necessitates an SAML token. Therefore, this cloud service grants user access via an authentication gate hosted by some other organization. An identity provider authenticates the cloud-user entity, which subsequently provides validated data through its services [18].

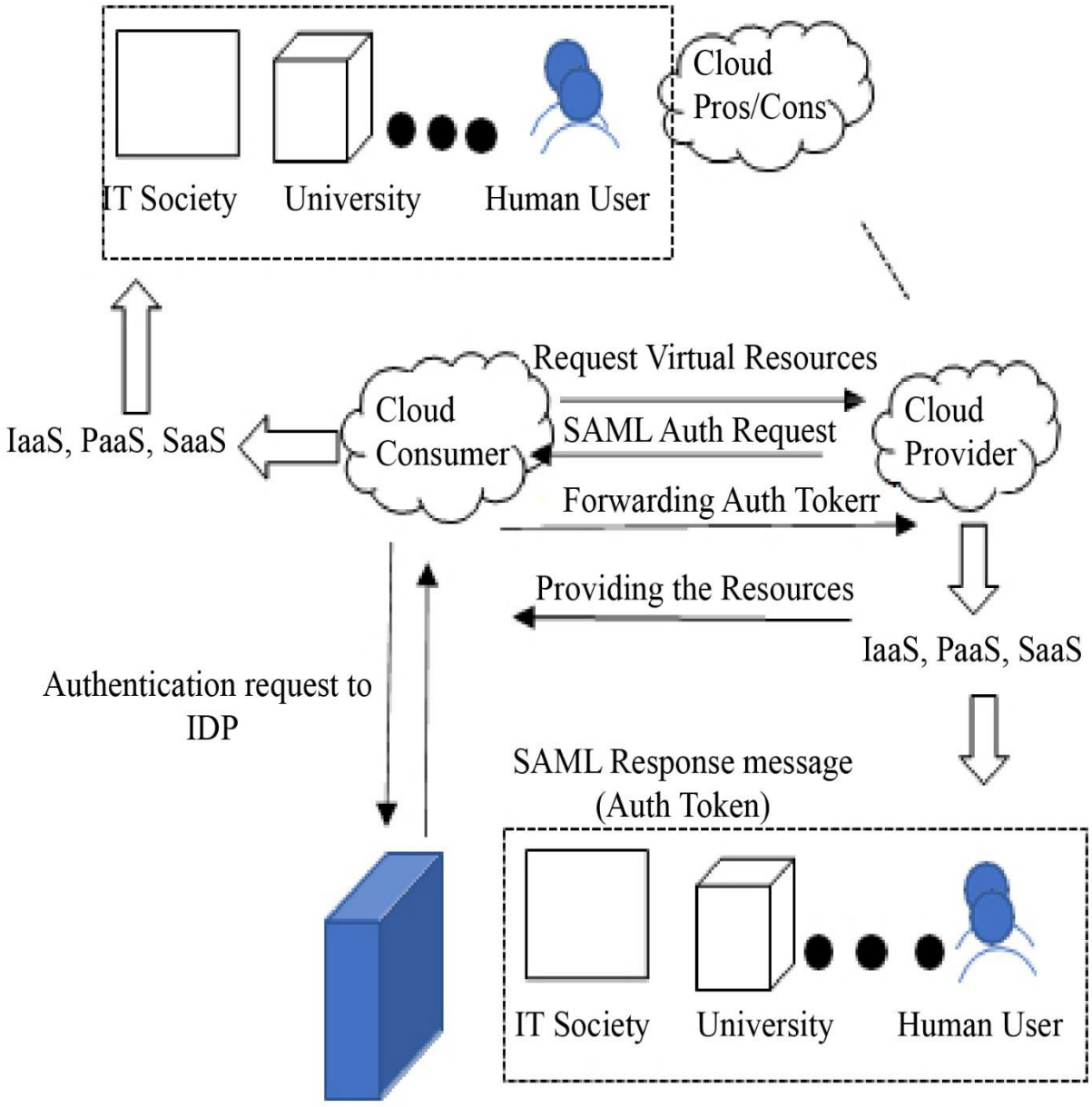

Fig. 5 SAML authentication

The cloud consumer redirects to their direct connection to the cloud and provides a resource request connecting to it, and the authentication token is acquired. Then, the cloud provider undoes the request containing the token and verifies its accuracy. Lastly, the cloud provider associates with the cloud consumer, informing them how and where to use the requested resources. The cloud consumer will send access to the resources of other cloud providers, trusting that an identity provider without further authentication works.

4.3. OAuth

OAuth is also known as Open Authentication, an open standard protocol that permits users to allow third-party applications to access their credentials without sharing passwords. The OAuth protocol is highly used in the IAM federation. It is highly used in mobile, desktop applications, and on the web [19]. OAuth has become the most widely used protocol because of its swift and high implementation in the industry [20]. The OAuth protocol is primarily designed to

provide a secure transport layer and approval layer for HTTP-based services. It provides many significant access management supports to users, businesses, and developers by protecting login data from unauthorized and restrictive access to other important information. It works when a person signs in on one platform and that platform requests an authorization token from another platform. The platform issues an authorization token to enable the User access to resources. The OAuth framework offers notable advantages over traditional authentication methods. It facilitates enhanced integration opportunities across applications. It has improved security and developed a user experience [19]. OAuth has decreased development effort and easy access to cancellation.

It also has disadvantages; it has difficulty implementing and always depends on a third-party service. If a third-party service offers OAuth operational experience issues, it will influence user access to applications that trust it. It will provide additional network requests, which can affect performance in many situations.

Fig. 6 Interaction between the four roles of the OAuth protocol flow

Figure 6 illustrates how the four functions within the OAuth protocol sequence interrelate. OAuth handles the scenario where trusted external entities can access users' authentic information securely. It delineates the functions of being a resource server, an authenticated user, and a data holder. The client submits an authorization request. The request can either go straight to the resource holder or pass via an intermediary such as the authentication service. Upon receiving an authorization token, the user signifies their agreement for access. Upon confirming the validity of the authentication token, the application transmits this information to the authorization endpoint. The authentication service checks the identity of the requester before granting access. Should approval be granted, the authentication service shall generate an access credential. Following the request for resources by the client, it subsequently obtains an access token, which is validated through authentication procedures on the resource server. When the token proves useful, it assists in completing the action requested by the system.

4.4. OpenID Connect

OpenID Connect is a way to check if someone is allowed to use different programs with just one login. It is also used in Identity and Access Management (IAM) federation. It is the most common Single Sign-On method that helps confirm a user's identity. Companies such as Amazon, Microsoft, Google, and PayPal utilize OpenID Connect. It helps with managing user identities, improves security, makes it easier to handle user accounts, and helps track how things work step by step. OIDC will develop security by confirming user identity details and offering confirmation. It will also streamline the IAM workflow by making things easier to verify and address security breaches. It has advantages in providing high-quality performance and creating a better user experience. It provides a whole homogeneous setup and makes friendly authentication. Even though it has many advantages, it also has disadvantages, such as a single point of failure, danger, and dependency on a third-party IDP. It has difficulty with maintenance and setup. OIDC implementation contains intricate outlines and continuing management of identity providers, mainly when it is handled with many applications and trust relationships. OIDC.

Figure 7 shows the OpenID Connect implicit flow. OIDC generally has some setup, in which the identity provider will register the RP (Relying party) and offer a set of URIs known as redirect URIs [23]. RP will send the ID tokens. The RP provides extra details like the name and ID. The IdP shows the user for login. As shown in Figure 6, the user needs to use their browser, which starts the process by asking for access to the RP. They choose the identity provider they want to use. Then, the RP sends the user's browser to the identity provider and asks for the client ID and a new time as part of the request. The user's browser then goes back to the identity provider and passes those details along. The IdP takes the information from the browser and asks the user to confirm they want to access

the RP using the client ID. The user clicks the confirm button, and the IdP sends back an ID token. The RP gets this ID token from the browser and checks if the signature on it is valid. It compares the signature with the client ID. If they match, the RP accepts the user and lets them log in successfully.

4.5. Attribute-Based Access Control (ABAC)

In IAM federation, attribute-based access control is defined as a system that is used to manage user access to resources based on dynamic attributes related to the resources, the environment, and the User. The ABAC method enables fine-grained authorization beyond simple RBAC by assessing multiple attributes to regulate access rights and relying on predefined roles.

This method is especially helpful while integrating the exterior identity providers, which will transfer user qualities by SAML assertion and allow flexible access control depending on particular user identities, such as location, job title, and department.

The ABAC method has several benefits in IAM federation [24]. It has improved high security, flexibility, and decreased administrative overhead. Among multiple attributes, this method provides granular access control and reduces unauthorized access. ABAC will easily adapt to access policies by adjusting business needs through changing attribute standards, without requiring the creation of new roles.

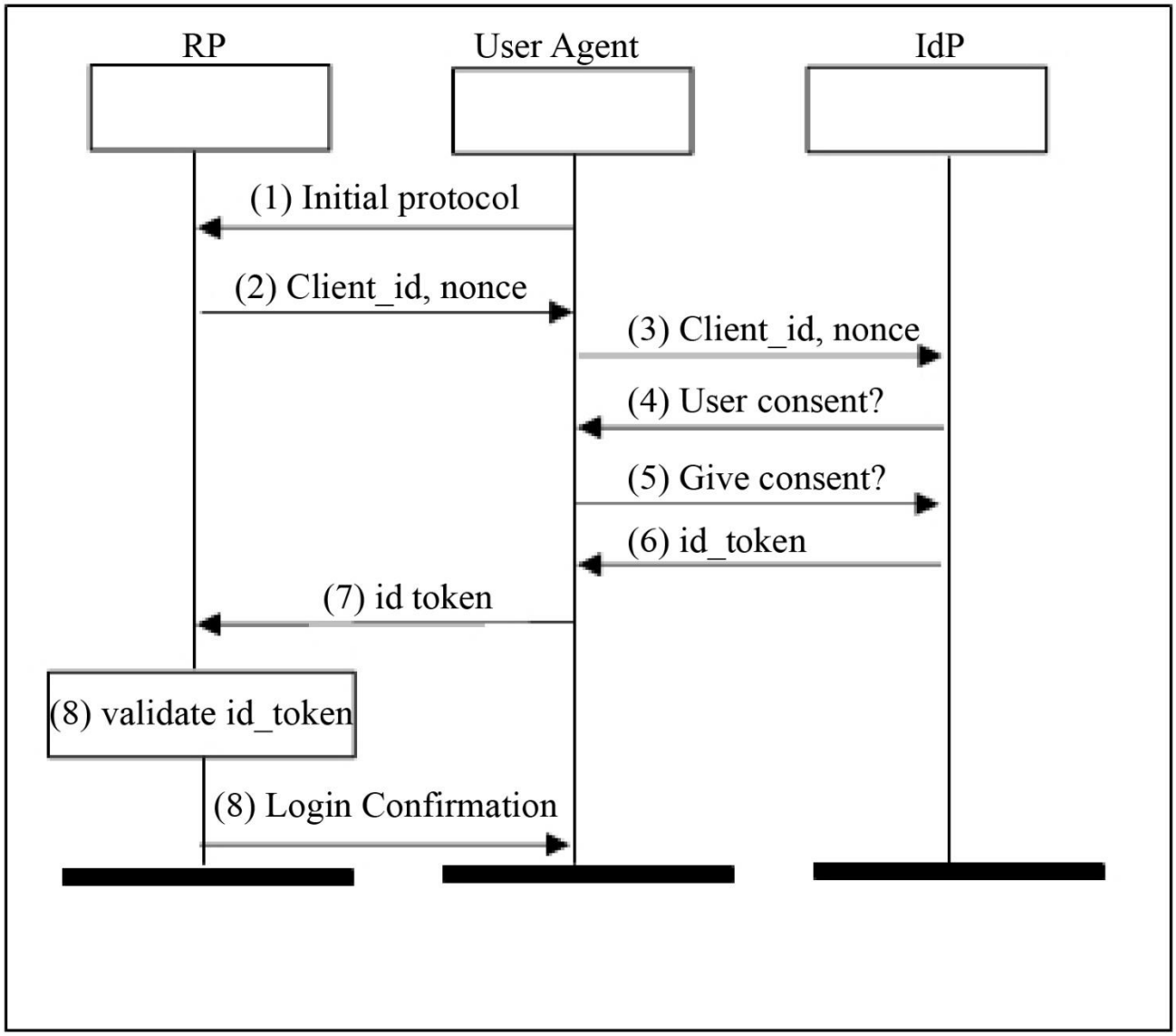

Fig. 7 OpenID connect implicit flow

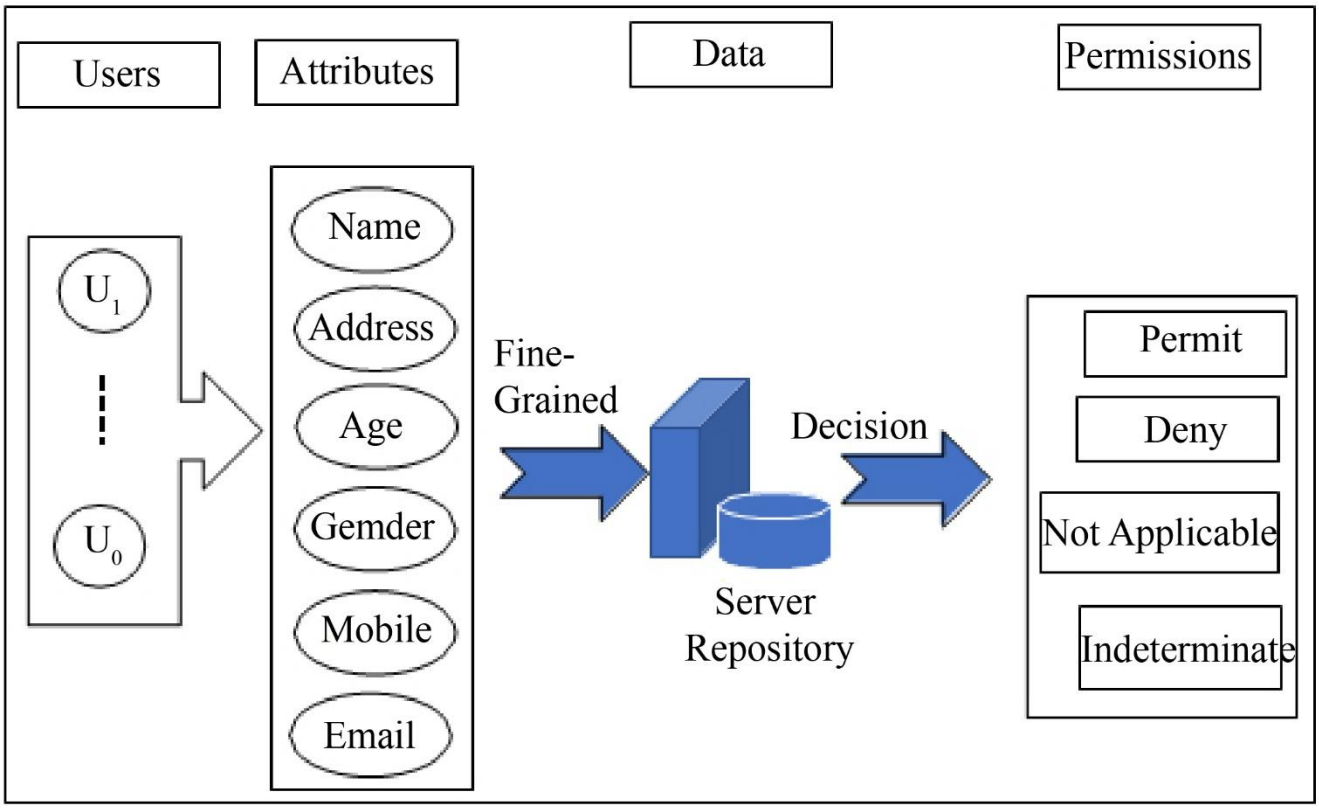

Fig. 8 Scheme of attribute-based access control

ABAC has dynamic access control, fine-grained permissions, scalability, and attributes from an identity provider. In IAM federation, ABAC methods have both advantages and disadvantages. ABAC has a disadvantage in that implementing and controlling ABAC will be difficult and requires a high level of consciousness of attributes and their connections, which generally leads to configuration mistakes [30]. It has auditing challenges because ABAC has a dynamic nature, which will require access control to depend on auditing, attributes, and tracking user activities, which will be difficult. It has many implementation challenges because it helps various protocol flows and expresses different SP types.

Figure 8 is a dataflow diagram that represents an attribute-based access control method. There is increasing interest in implementing an attribute-based access control design for data privacy. The ABAC model is intended to offer greater control over data access, ensuring it is more accurate and secure. Figure 7 highlights that each user's attributes, such as name, address, mobile number, age, time, and location, determine their access to system resources. This model aims to manage user attributes to provide more informative and reliable access to data. It is intended to offer greater control over data access, ensuring it is more accurate and secure. This model will provide permission to the User after fine-grained through the server repository and make a decision about whether the User will permit, deny, not applicable, or indeterminate. The attributes of ABAC are divided by object, action, environment, and subject.

4.6. Kerberos

Kerberos is the secure authentication protocol that is mainly used in Identity and Access Management (IAM) federation [32]. It permits users to use multiple services through various domains by using a single login. Kerberos protocol mainly offers single sign-on functionality by applying the encoded tickets that are issued by the KDC, the central key distribution center. This protocol will remove the necessity of repeatedly entering the user credentials to access all services.

In recent days, many organizations have adopted the Kerberos protocol, including versions four and five. In the IAM federation, the Kerberos protocol consists of three components, which are the client, the key distribution center, and the server [31]. Kerberos is generally defined as a ticket-based system intended to provide strong authentication for server and client applications through the use of secret key cryptography. The client looks at the ticket and uses it to get more tickets for accessing the network service. The main parts needed for the Kerberos protocol in IAM federation are the workstation, client, key distribution center, and credential cache. It has an advantage in IAM federation by improving highly secure authentication. Users will accept the Ticket-Granting Ticket (TGT) from the KDC after primary

verification, which allows them to send requests to service tickets for definite services without entering their password again. It developed security, centralized management, and an easier user experience. It is difficult to implement, and it relies on a synchronized time limit between the server and client. Kerberos is good for authentication in a single login, but it is also difficult to establish a reliable connection between client and server.

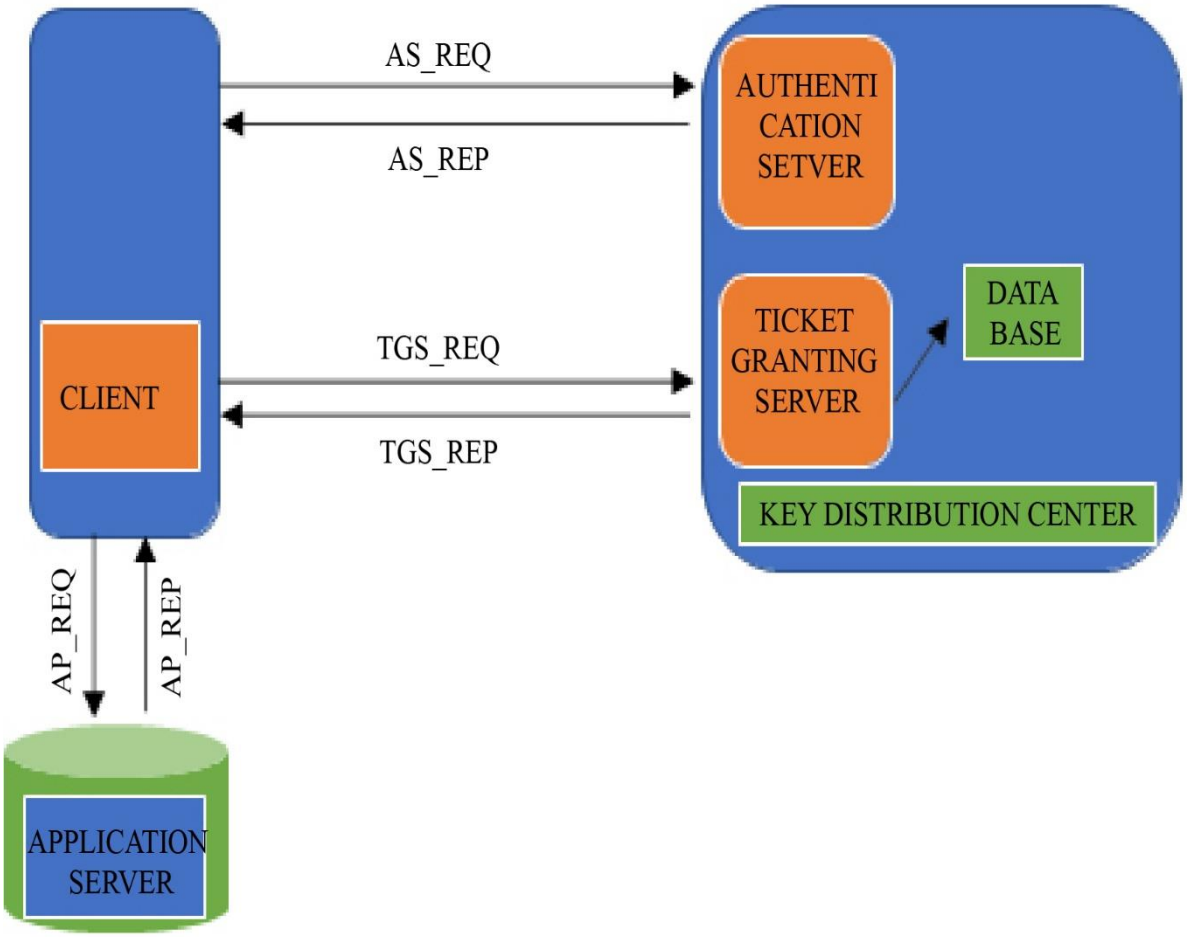

Fig. 9 Kerberos protocol working

Figure 9 illustrates the functioning of the Kerberos authentication mechanism. Referencing the illustration provided, initially, the user requests authorization services from the verification center before obtaining an access token. Subsequently, the verification center verifies an individual's credentials against its records before granting access tokens. When the customer receives the support request, they have access to services via the application server. Kerberos terminology refers to the Ticket Granting Service acting as TGS for tickets, clients functioning as C, applications on servers represented by Ap, client IPs indicated by Ip-lists, authenticators serving as AS, and applications also known as AP. The repository holds crucial data for clients. Client types its client ID and password, then sends a request for a workstation about service, and converts its private key. Then, the work workstation passes the information to an authentication server and sends the request for a ticket-granting ticket. The authentication server interprets the client request by directing the user to the user key in its database if a match is found. The workstation will decode the received message using its key, obtain a session key and TGT, and save them in the credential storage. Next, when the operator wants to access the workstation, the client application constructs an authenticator to make a request for ticket TGS, which includes the client's information.

The client application demands a server for service involving the received ticker and authenticator. Next, the service validates the request by interpreting the session key. It confirms whether the authenticator and ticket match or not, and then grants permission to the service if a match is found. In the end, mutual authentication is mandatory. The server should send a reply with the help of a server authentication message.

4.7. System for Cross-domain Identity Management (SCIM)

SCIM is the provisioning protocol that is highly used in IAM federation [33]. It is the automated process of generating, updating, and deleting user accounts within the identity and access management federation. This process of generating, updating, and removing is completed by the system of the cross-domain identity management protocol. It permits the unified synchronization of user data between the IdP and the IAM system. This protocol also handles user access between various applications inside the federated environment. SCIM uses the homogeneous REST API to connect user data between the identity and access management and identity provider systems by confirming compatibility between different platforms. In IAM federation, SCIM has benefits by improving efficiency. Automatic user provisioning will help decrease the administrative overhead. It also helps in increasing security. SCIM confirms the exact user access by mechanically updating account data when changes happen in the IdP. IT has benefits in scalability. It supports a large measure of user management between various applications. SCIM works through configuration, mapping, and synchronization. SCIM protocol in IAM federation has some disadvantages, including filtering and attribute limitations. SCIM REST API will be vulnerable to attacks that occur due to unauthorized access to systems, applications, and data. Another disadvantage is that if SCIM solutions are implemented poorly, then it will affect the app to overflow with requests, and it will bring the system down. SCIM handling is not common, and the experience of using SCIM will change greatly from vendor to vendor.

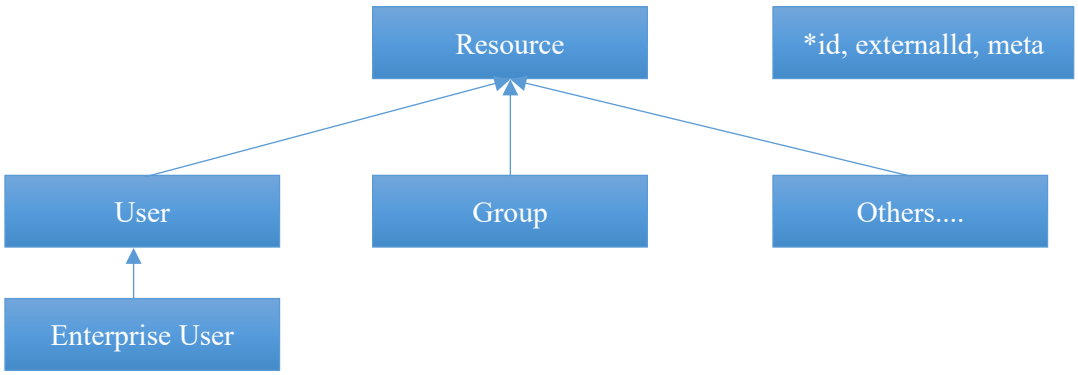

Fig. 10 SCIM model

Figure 10 shows the system for the cross-domain identity management model. The SCIM protocol generally practices a tree model to express what attributes are required in a resource. This model shows that the resources have a child-parent relationship in Figure 9. SCIM protocol not only regulates the allowance to make the resources, but it also explains how to get all the qualities from parent resources. The root node is known as resources, and it is kept inside the common attributes. The common attributes are resource name, and the complex attributes are id, extra id, and meta [34]. The ID is the single identifier provided by the service provider to resources for tracking purposes. It cannot be null and has unique characteristics. The external ID is one of the identifiers that specifies the resources are in the client system. Meta is the last common attribute and resource Type; location and version are its sub-attributes. The service provider maintained this metadata for all the resources. As per the diagram, resources are divided into User, group, and others. If all the credentials match, then the service provider gave access for the applications.

4.8. WS Federation

In IAM federation, WS federation is defined as the standardized protocol that is used to qualify single sign-on between various security domains by permitting users to validate with one identity provider and access many different applications without reentering passwords or other credentials. The main focus of WS federation is to simplify the federated service development by cross-domain connection and controlling federated services by reclaiming the WS trust security token service model and protocol. Many types of federated services, such as authorization, authentication, and attributes, are improved by the difference in the base security token service. It has high benefits in IAM federation because WS federation works as a device for transferring identity data between trust domains through safe communication. It is the main technology for executing federated verification inside the IAM system, especially for web applications. WS federation provides a path for STS (Security Token Services) in one domain to offer authentication permits to an STS in another trusted domain. It allows users to use the application across various organizations through a single set of credentials. WS federation influences other web services standards, such as WS-Trust and WS-Security, to protect the transfer of identity data by SOAP messages. It has advantages by helping both passive and active clients, and a unified combination with Microsoft applications. It gave a strong security mechanism because of its XML nature protocol. The main disadvantage of WS Federation is its dependence on a third-party provider, limited flexibility, and difficulty in application and configuration.

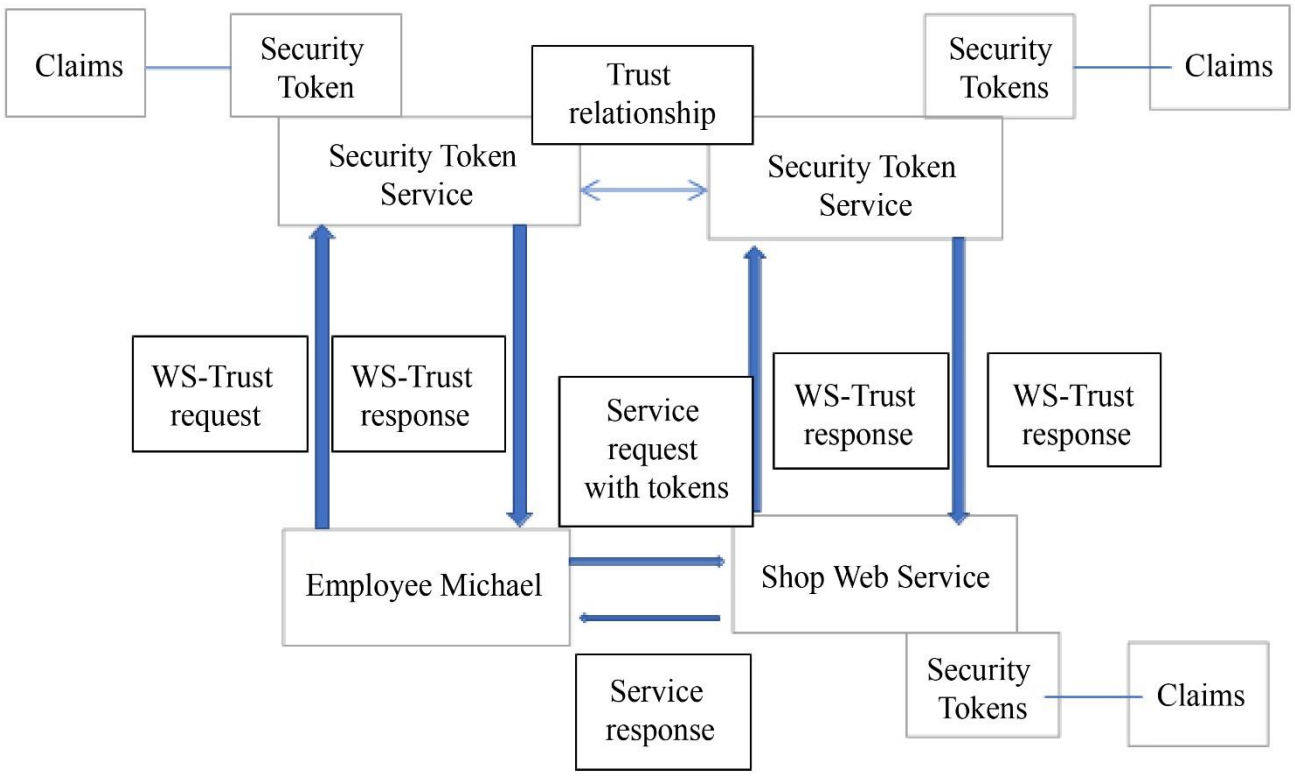

Fig. 11 WS-federation and WS-trust

Figure 11 shows how WS Federation works. The Security Token Services (STS) are defined as the basic service that exchanges the security tokens by using a common set of messages and models. As per the figure, the employee will send the WS trust request to the STS. Then the STS verifies the user access and exchanges the security token using the basic model.

The STS was to rise and clarify the ticket and manage security tokens. It works as the trusted third party that is created between the web service provider and the requester. WS-Trust frequently exchanges the tokens and supports building trust relations by applications, permitting them to request, renew, issue, and clarify security tokens for authentication services. The SHOP web service sends a request to WS-Trust, and WS-Trust responds by returning the token after verification.

This process is exchanging the tokens for authentication, and in the end, it claims the token after verifying each party's identity. Table 2 shows that Single Sign-On (SSO) is more usable as the user can use the same set of credentials to gain access to numerous platforms, and on the other hand, it also has a risk of a single point of failure in the event of an attack. This may be addressed with Multifactor Authentication (MFA), which is more secure but may be inconvenient because of extra interactions during the process of logging in. OAuth is very scalable, and most third-party access is done without sharing credentials, but it is complicated to use by users, particularly in the handling of the authorization tokens. Privileged Access Management (PAM) plays an essential role in the control of access to sensitive data, especially in the regulated sectors, but it is expensive and complicated to maintain. SAML is highly secure in terms of enterprise-level SSO, but it is less scalable compared to OpenID Connect, which is more scalable and easier to set up, especially in the cloud. Nevertheless, OpenID Connect is also based on third-party identity providers, which poses a vulnerability in the event that such providers are attacked.

4.9. Ethical Implications

Although IAM tools are associated with important advantages in terms of security and convenience, they also pose important ethical issues. Privacy of users is one of the foremost factors for IAM systems, since these systems are often concerned with sensitive identity data. Organizations must take steps to validate that they are using sufficient data protection in their operations and limit the amount of personal data they collect from users to try to mitigate privacy concerns. The governance of data is another major issue, due to the increasingly strict data regulations emerging, including GDPR and HIPAA requirements. IAM systems must allow organizations to be in compliance with these regulations to ensure that sensitive data is secured and users manage access to resources safely.

Table 2. Comparative analysis of IAM tools

Tool	Security	Usability	Scalability	Compliance
SSO	High – Reduces password fatigue, but risks a single point of failure.	Very High – One credential for multiple applications.	High – Easily integrates with multiple apps.	GDPR, HIPAA, and FERPA are compliant with proper implementation.
MFA	Very High – Adds multiple layers of authentication for enhanced security.	Moderate – Can be inconvenient for users due to additional steps.	High – Compatible with a variety of authentication methods.	High – Ensures compliance with data protection regulations.
OAuth	High – Provides delegated access without exposing credentials.	Moderate – Slightly complex for end users to fully understand.	Very High – Widely adopted across platforms.	Compliant with GDPR when used properly for consent and data access.
PAM	Very High – Restricts and monitors privileged accounts, reducing insider threats.	Moderate – Complex to implement, high administrative overhead.	Moderate – Suitable for organizations with extensive privileged accounts.	Ensures compliance with internal policies, HIPAA for healthcare.
SAML	High – Strong security assertions and protocols.	Moderate – Often requires specific configurations.	Moderate – Best suited for enterprise environments with fewer applications.	Very High – Supports GDPR and other compliance regulations.
OpenID Connect	High – Integrates with OAuth for user authentication.	High – Reduces complexity and improves the user experience.	High – Scalable for large distributed systems.	Supports GDPR and FERPA with adequate privacy safeguards.

5. Experimental Results and Analysis

5.1. Overview of Evaluation

For comparing functionality of some of the most popular Identity and Access Management (IAM) federation methods, six of the most commonly used ones such as Single Sign-On (SSO), Multifactor Authentication (MFA), OAuth, Privileged Access Management (PAM), Security Assertion Markup Language (SAML), and OpenID Connect were compared on four criteria: Security, Usability, Scalability, and Compliance.

The assessment framework is a combination of qualitative and quantitative approaches, drawing upon secondary evidence from peer-reviewed research, standards documentation (e.g., SAML, OAuth, OpenID Connect, GDPR, HIPAA), and industry case studies. Each tool was examined for its capacity to provide secure, compliant, and interoperable identity management in federated contexts.

5.2. Quantitative Evaluation and Results

Table 3 shows the comparative percentage scores of each IAM tool for the four evaluation criteria. The Overall Score is a straightforward arithmetic mean of the four criteria, which represents the overall performance and usability of the tool in federated IAM environments.

Table 3. Comparative evaluation of IAM tools

Tool	Security (%)	Usability (%)	Scalability (%)	Compliance (%)	Recalculated Overall (%)
SSO	90	95	85	92	90.5
MFA	95	75	90	94	88.5
OAuth	85	80	95	90	87.5
PAM	98	70	80	95	85.75
SAML	92	78	80	98	87.0
OpenID Connect	90	88	93	94	91.25

Six IAM mechanisms, SSO, MFA, OAuth, PAM, SAML, and OpenID Connect, are depicted on the four performance criteria of security, usability, scalability, and compliance in Figure 12 and depict the unique strengths and tradeoffs of each. Figure 13 represents the recalculated scores of overall efficiency, best for OpenID Connect and SSO, based on balanced efficiency and interoperability. Figure 14 illustrates the correlation among the factors of evaluation, demonstrating positive correlations between security and compliance and negative correlations between scalability and compliance, which overall demonstrate how enhancements in one feature may affect others in federated IAM systems.

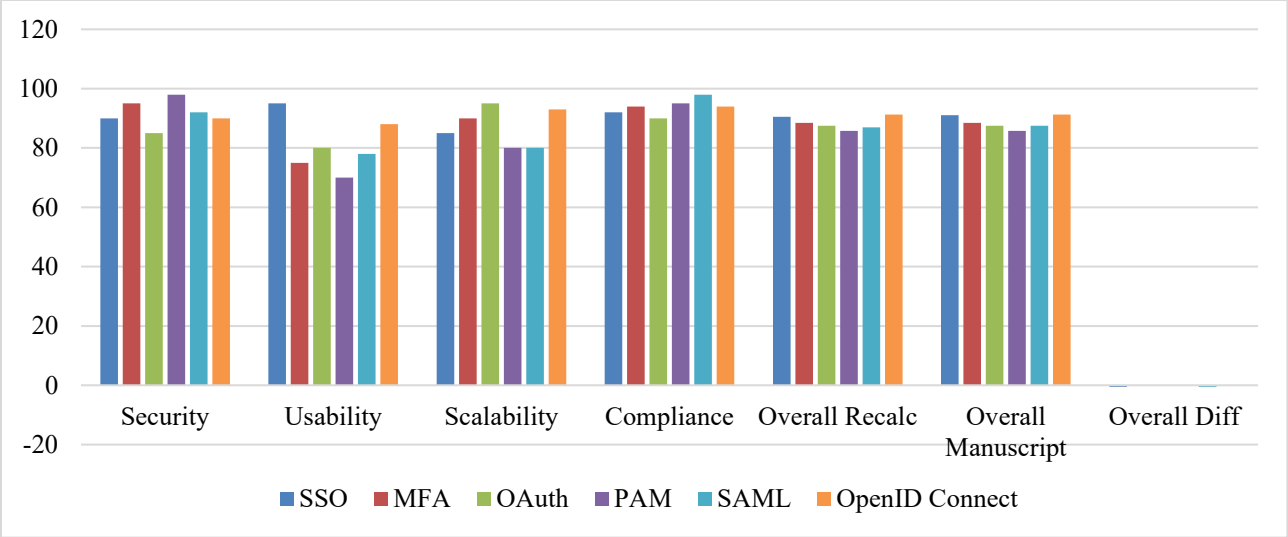

Fig. 12 Comparative analysis of IAM tools based on security, usability, scalability, and compliance.

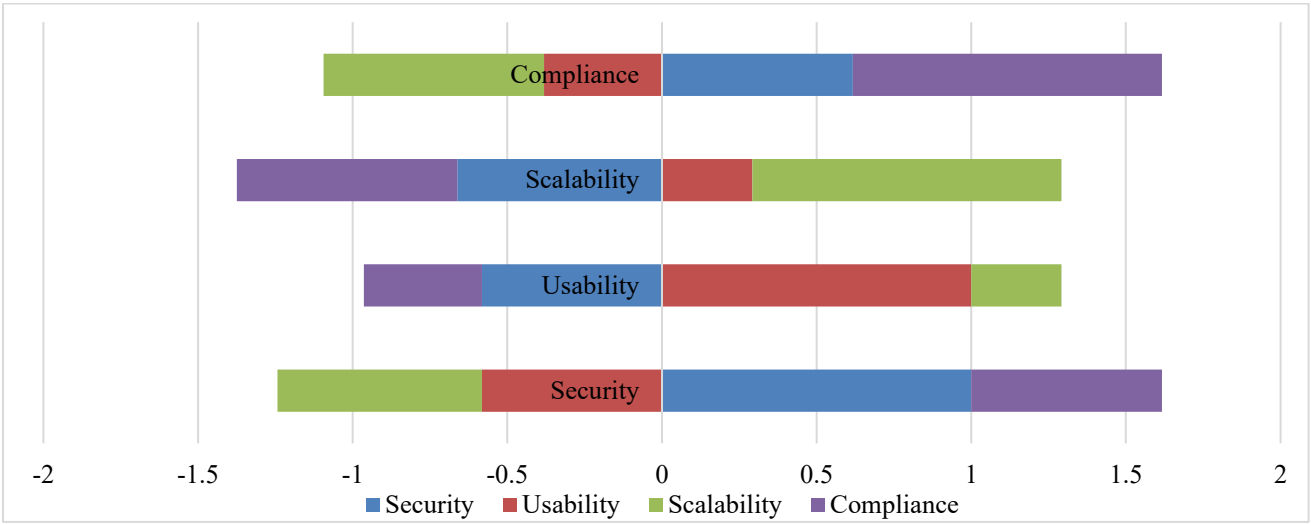

Fig. 13 Overall performance ranking of IAM federation tools

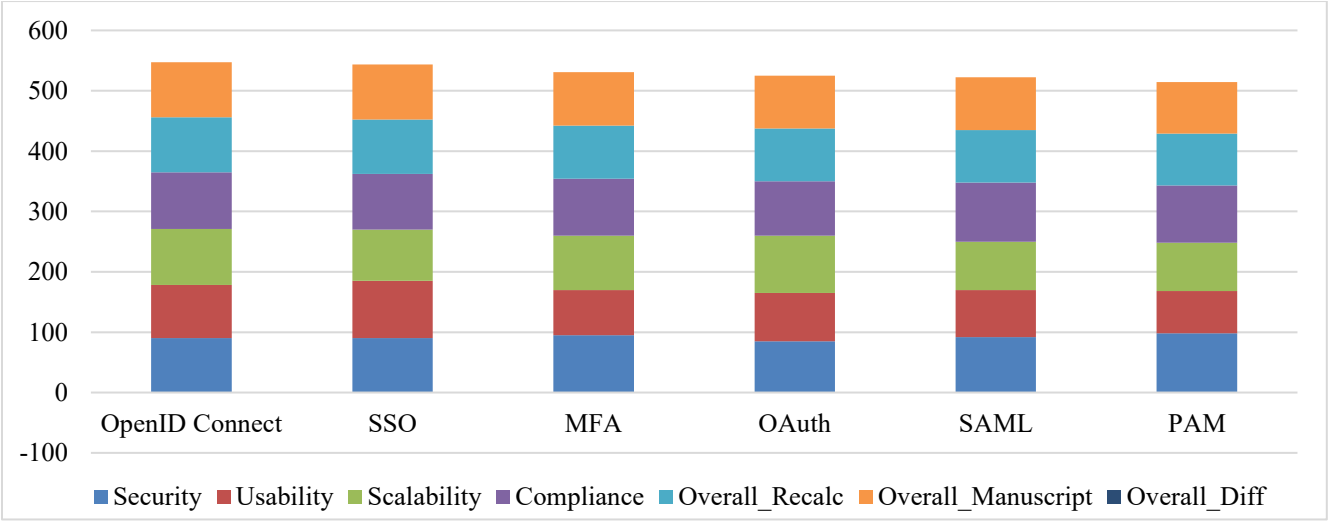

Fig. 14 Correlation matrix between IAM evaluation criteria

5.3. Analysis and Interpretation

The outcomes show that Single Sign-On (SSO) and OpenID Connect have the highest overall ratings (90.5% and 91.25%, respectively) because they provide the optimal tradeoff between usability, scalability, and regulatory compliance. Privileged Access Management (PAM) gets the highest security ranking (98%) but worse overall performance ratings because it gets lower usability (70%) and scalability (80%) ratings. MFA is very secure (95%) but less convenient because it involves more authentication steps. OAuth is very scalable (95%) and interoperable, but it relies on third-party services, which may not be reliable in the long term. SAML is secure and compliant, but less scalable because it has a verbose XML format. Correlation analysis determines Security and Compliance to be positively correlated ($r = 0.62$), demonstrating that stricter security controls have a tendency to result in favorable regulatory compliance. Compliance and Scalability are moderately negatively correlated ($r = –0.71$), demonstrating that high mechanisms of compliance sometimes tend to decrease flexibility and performance in large systems. Generally, the review determines that OpenID Connect and SSO are the most evenly balanced solutions for federated spaces, while PAM and MFA are best suited for high-security or regulated industries.

5.4. Implications for IAM Federation

The comparative review is indicative of the necessity for hybrid IAM architectures that marry usability, scalability, and security in Zero-Trust paradigms. The combination of AI-based adaptive authentication, blockchain-protected audit trails, and context-aware access controls further supports the robustness and transparency of federated identity systems. The findings offer evidence-based grounds for organizations to choose IAM frameworks that are commensurate with their business size, compliance requirements, and risk levels.

5.5. Directory-Based IAM Solution Comparison Overview

Apart from federated identity protocols such as SAML, OAuth, and OpenID Connect, enterprise identity management also heavily relies on directory-based platforms, including Microsoft Active Directory (AD), OpenLDAP, and Azure Active Directory (AAD). These environments are the underlying storehouses of user credentials, access policies, and authentication processes. Active Directory (AD) offers authentication and policy management within Windows environments via centralized access, including support for integrating secure access via Kerberos and LDAP. OpenLDAP is an open-source, highly customizable option that allows federation via external identity brokers, but requires greater administrative expertise. Azure Active Directory (AAD) extends directory services into the cloud with native support for OAuth 2.0, OpenID Connect, and SAML, and it is straightforward to set up hybrid and cloud-based IAM installations. In short, AD is the choice for traditional enterprise environments, OpenLDAP is better suited for open and customizable environments, and AAD offers an extensible and unified solution for hybrid environments.

6. Conclusion

This article illustrates the strengths and weaknesses of various IAM solutions: SSO, MFA, OAuth, PAM, SAML, and OpenID Connect. All the tools are strong to considerably strong in providing additional security and user experience functionalities, yet they have tradeoffs, especially in terms of user experience and security measures. SSO and MFA are particularly strong in compliance, while OAuth and OpenID Connect's strengths lie in scalability, particularly for cloud-based applications, but there are still scalability issues, complexity of foundations, identity providers in the cloud, and the separation of enterprise applications.

PAM is absolutely required in the high-security space, yet it is expensive and operationally complex. The article suggests that, in the end, developers need to improve the user experience in MFA by minimizing friction, utilizing Artificial Intelligence for real-time threat detection, and leveraging blockchain technology, which would enhance data privacy and transparency in federated Identity Access Management. New Zero Trust forms and adaptive access control can provide a more dynamic and resilient IAM that is more suited to the new digital age.

References

[1] Sampath Talluri, "Identity and Access Management for the Internet of Things (IoT)," *Journal of Engineering and Applied Sciences Technology*, vol. 4, no. 1, pp. 1-4, 2022. [Publisher Link]

[2] Amjad Alsirhani, Mohamed Ezz, and Ayman Mohamed Mostafa, "Advanced Authentication Mechanisms for Identity and Access Management in Cloud Computing," *Computer Systems Science and Engineering*, vol. 43, no. 3, pp. 967-984, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Chetanpal Singh, Rahul Thakkar, and Jatinder Warraich, "IAM Identity Access Management-Importance in Maintaining Security Systems within Organizations," *European Journal of Engineering and Technology Research*, vol. 8, no. 4, pp. 30-38, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Daniela Pöhn, and Peter Hillmann, "Reference Service Model for Federated Identity Management," *International Conference on Business Process Modeling, Development and Support*, Melbourne, VIC, Australia, pp. 196-211, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] None Saloni Kumari, "Identity and Access Management: "Elevating Security and Efficiency: Unveiling the Crucial Aspects of Identity and Access Management"," *International Journal of Engineering & Technology*, vol. 12, no. 1, pp. 11-14, 2023. [Publisher Link]

[6] Prashant Pandey, and T.N. Nisha, "Challenges in Single Sign-On," *Journal of Physics: Conference Series: Advances in Computer Science Engineering*, vol. 1964, no. 4, pp. 1-12, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] Swapnoneel Roy, Sam Matloob, and Debajyoti Mukhopadhyay, "On Application of Blockchain to Enhance Single Sign-On (SSO) Systems," *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Shenyang, China, pp. 1191-1195, 2021. [Google Scholar] [Publisher Link]

[8] Anna Schlenker, and Milan Šárek, "Behavioral Biometrics for Multifactor Authentication in Biomedicine," *European Journal for Biomedical Informatics*, vol. 8, no. 5, pp. 19-24, 2012. [Google Scholar] [Publisher Link]

[9] Muhammad Aslam, "The Impact of Multi-Factor Authentication (MFA) on Strengthening Cybersecurity in E-Commerce Applications," 2020. [Google Scholar]

[10] Ayman Mohamed Mostafa et al., "Strengthening Cloud Security: An Innovative Multifactor Multi-Layer Authentication Framework for Cloud User Authentication," *Applied Sciences*, vol. 13, no. 19, pp. 1-24, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] K. Krishna Prasad, "Multifactor Authentication Model using Fingerprint Hash Code and Iris Recognition" *International Journal of Management, Technology, and Social Sciences (IJMTS)*, vol. 3, no. 2, pp. 47-56, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[12] Alexander D. Kent, Lorie M. Liebrock, and James Wernicke, "Differentiating User Authentication Graphs," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 5, no. 2, pp. 24-38, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[13] Swetha Gadde et al., "Secure Data Sharing in Cloud Computing: A Comprehensive Survey of Two-Factor Authentication and Cryptographic Solutions," *Information Systems Engineering*, vol. 28, no. 6, pp. 1467-1477, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Iryna Topalova et al., "Business Process Management in Entrepreneurial Activity Based on a Platform Approach," *Indian Journal of Information Sources and Services*, vol. 14, no. 2, pp. 46-55, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[15] Srikanth Mandru, "Privileged Access Management and Regulatory Compliance," *Journal of Artificial Intelligence, Machine Learning and Data Science*, vol. 2, no. 2, pp. 728-732, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] André Koot, "Introduction to Privileged Access Management (v2)," *IDPro Body of Knowledge*, vol. 1, no. 15, pp. 1-21, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] Ifteher Alom et al., "Dynamic Management of Identity Federations using Blockchain," *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Sydney, Australia, pp. 1-9, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] Amani K. Samha, "Strategies for Efficient Resource Management in Federated Cloud Environments Supporting Infrastructure as a Service (IaaS)," *Journal of Engineering Research*, vol. 12, no. 2, pp. 101-114, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] Srivathsan G. Morkonda, Paul C. van Oorschot, and Sonia Chiasson, "Exploring Privacy Implications in OAuth Deployments," *arXiv Preprint*, pp. 1-15, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Sasibhushana Matcha, and Munish Kumar, "Enhancing Software Security with OAuth 2.0: Implementation Strategies and Vulnerability Mitigation," *Journal of Emerging Technologies and Innovative Research*, vol. 12, no. 3, pp. e886-e902, 2025. [Google Scholar] [Publisher Link]

[21] Seyyed Keyvan Mousavi et al., "Security of Internet of Things based on Cryptographic Algorithms: A Survey," *Wireless Networks*, vol. 27, no. 2, pp. 1515-1555, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[22] Louis Jannett et al., "Sok: SSO-MONITOR-The Current State and Future Research Directions in Single Sign-on Security Measurements," *2024 IEEE 9th European Symposium on Security and Privacy (EuroS&P)*, Vienna, Austria, pp. 173-192, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[23] Sven Hammann, Ralf Sasse, and David Basin, "Privacy-Preserving OpenID Connect," *ASIA CCS '20: The 15th ACM Asia Conference on Computer and Communications Security*, Taipei, Taiwan, pp. 277-289, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[24] Santripti Bhujel, and N. Priya, A Review of Identity and Access Management as a Service, 2021. [Online]. Available: https://www.researchgate.net/publication/351810416_A_REVIEW_ON_IDENTITY_AND_ACCESS_MANAGEMENT_AS_A_SERVICE?channel=doi&linkId=60ab2b61299bf1031fc41d96&showFulltext=true

[25] Jana Glöckler et al., "A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity," *Business & Information Systems Engineering*, vol. 66, no. 4, pp. 421-440, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[26] Omer Eltayeb, "The Crucial Significance of Governance, Risk, and Compliance in Identity and Access Management," *Journal of Ecohumanism*, vol. 3, no. 4, pp. 2395-2405, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[27] Andrew Cormack, "An Introduction to the GDPR (v3)," *IDPro Body of Knowledge*, vol. 1, no. 5, pp. 1-13, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[28] Michal Maciej Kepkowski, "*Privacy-Enhancing Technologies for Identity and Access Management*," Doctoral Dissertation, Macquarie University, 2024. [Google Scholar] [Publisher Link]

[29] Tom Petersen, "*Distributed Architectures for Data Pseudonymization and Anonymization in Medical Research*," Doctoral Dissertation, University of Hamburg, 2024. [Google Scholar] [Publisher Link]

[30] Javed Akhtar Khan, *Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC)*, Improving Security, Privacy, And Trust in Cloud Computing, IGI Global Scientific Publishing, pp. 113-126, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[31] Santosh Kumar Singh, Priyanka Dubey, and Gyanendra Kumar Shukla, "MongoDB in a Cloud Environment" *Don Bosco Institute of Technology Delhi Journal of Research*, vol. 1, no. 1, pp. 13-18, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[32] Thomas Baumer, Mathis Müller, and Günther Pernul, "System for Cross-Domain Identity Management (SCIM): Survey and Enhancement with RBAC," *IEEE Access*, vol. 11, pp. 86872-86894, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[33] Morey J. Haber, and Darran Rolls, *System for Cross-Domain Identity Management (SCIM)*, Identity Attack Vectors, Apress, Berkeley, CA, pp. 159-161, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[34] Mersedeh Sadeghi, "Interoperability of Heterogeneous Systems of Systems: from Requirements to a Reference Architecture," *The Journal of Supercomputing*, vol. 80, no. 7, pp. 8954-8987, 2023. [Google Scholar] [Publisher Link]