International Journal of Core Engineering & Management
Volume-6, Issue-12, 2021 ISSN No: 2348-9510

SAML VS. LDAP: BEST PRACTICES AND USE CASES FOR CLOUD-BASED ENTERPRISE AUTHENTICATION AND AUTHORIZATION

Dhaval Gogri
dhaval.gogri17@gmail.com

Abstract

The modern society consumes one product using many applications which hence requires the user to authenticate each application. This sometimes requires handling of different username and passwords for different service providers. As more and more digital services are being introduced therefore the need for sound and secure methods of authentication and authorization increasingly gets felt. In the current fast-changing technological environment, strong technologies for authentication and authorization play a crucial role in securing significant enterprise information and ensuring the stability of the enterprise. SAML and LDAP are well known protocols implemented in cloud-based systems for identity management. This review paper is concerned with identifying and comparing the characteristics, strengths, weaknesses, and potential applications of SAML and LDAP in cloud-based enterprise applications. We go into the SAML and LDAP architectures, explaining why and how these standards may meet the authentication and authorization needs of the future with solutions for SSO, directory services, and cloud-native integration, among other things. Further, we describe how to apply each of the protocols to provide better security and convenient for the users' experience. Our main intention for this review is to assist IT practitioners, system designers, as well as cybersecurity specialists to identify a suitable protocol that responds to enterprises' demands, security constraints, and scalability.

Keywords: SAML, LDAP, Cloud Security, Authentication, Authorization, Identity Management, Cloud Computing.

I. INTRODUCTION

Authentication and authorization constitute the basis of cloud storage security in cloud computing, which is a widely used and popular kind of computing that promises great dependability for both clients and suppliers in many industries [1]. There are two main issues when it comes to users accessing data stored in the cloud from the data centre: authentication and authorization. Data is uploaded into the cloud and kept in databases [2]. Managing user identities and credentials in relation to an organization's technological resources is a challenging issue that many businesses are now facing. The evolution of Internet technology has favourably influenced various domains. This also facilitates the creation of web-based applications necessary for governmental entities, corporate sectors, and educational institutions. User identity requirements have become a critical problem in accordance with the trend of utilizing online apps for corporate operations and security standards [3]. The management of users and the development of infrastructure that complies with security standards have become critical elements [4][5].

Client-server applications on web servers have achieved extensive adoption and are experiencing

considerable growth. The significance of data confidentiality and user authentication has markedly increased [6]. Data integrity is an essential element of information security, protecting against unauthorized modifications, fabrication, and deletion. The establishment of authorization protocols is an important concern in a Cloud environment. Each authenticated user's access rights are defined and enforced via authorization. It is critical to ensure that only authorized organizations may access the protected data, nevertheless, since there are so many access points and system entities. A prevalent technique employed to guarantee integrity is the utilization of digital signatures [7]. The whole authentication strategy in cloud systems is shown in figure 1.

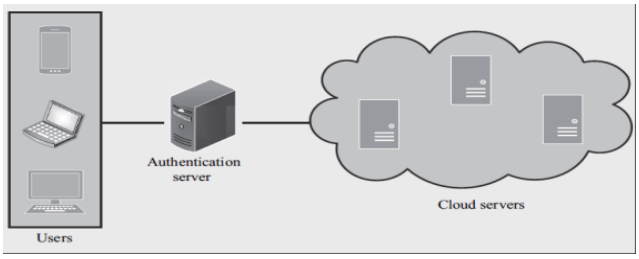

Fig. 1. The general authentication scheme in the cloud systems

Cloud computing authentication is guaranteed if the cloud's resources are accessed; in this case, the user's identity is provided to the cloud service provider [8]. The authentication methods that a cloud provider may pick from and provide have varying degrees of security granularity [9][10]. The strength of these systems is determined by their dependability and integrity [11]. The effective storage and manipulation of massive amounts of data on servers has emerged as a key concern for the business, despite the advancements in technology [12].

Cloud-based enterprise authentication and authorization often rely on protocols like SAML and LDAP to manage user access. SAML is commonly used for cloud environments, enabling Single Sign-On (SSO) through an identity provider that authenticates users once and grants access to multiple web applications with a single set of credentials. However, LDAP is actually a protocol which is used mostly in on-premises systems to access the directory information services which is the users and groups [13].

This paper focuses at comparing SAML and LDAP, two common protocols that are used in cloud environments for logistics of authentication and authorization. With the ever-growing adoption of cloud services there is always a need to determine the most appropriate security measures that guarantee secure access to systems and information. Therefore, the motivation behind this review is to help the enterprises deal with challenges of choosing the right identity management solution which meets their security and scalability needs and is also easy to integrate. This paper aims to assist IT decision-makers in the study of the relative advantages and disadvantages of SAML and LDAP to select the most appropriate protocol complementing their architecture in the future.

This review paper is structured into the following sections: Section I provides an introduction to the topic, Section II discusses cloud-based enterprise authentication and authorization, Section III explores the SAML, Section IV examines the LDAP, Section V analyses SAML and LDAP use cases for cloud-based enterprise authentication and authorization, Section VI presents a literature review, and Section VII concludes with findings and future work.

International Journal of Core Engineering & Management
Volume-6, Issue-12, 2021 ISSN No: 2348-9510

II. CLOUD-BASED ENTERPRISE AUTHENTICATION AND AUTHORIZATION

The concept of cloud computing, a novel approach to data storage and processing, has advanced rapidly in the last few years. Cloud computing has emerged as a large-scale IT service paradigm for dispersed network environments, made possible by the rapid expansion of service providers and the widespread availability of online resources. As a self-service utility, cloud computing is based on pre-existing Internet technology. There are three different service models: SaaS, IaaS, and PaaS. When it comes to commercial system deployment, the top cloud computing companies are Google, Microsoft Azure Platform, and Amazon Web Services. It doesn't matter which service type is used; cloud systems might be public, community, private, or hybrid. Cloud storage and security relies on several key elements, including privacy, authenticity, authorization, accounting, confidentiality, and auditing. Cloud security vulnerabilities are shown in figure 2.

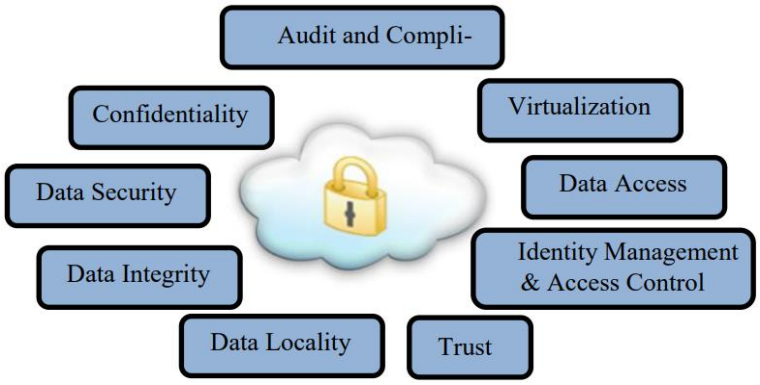

Fig. 2. Cloud security issues

The paradigm of the cloud service is quite important when it comes to cloud computing security. The most popular method of authentication, which is a key security service, involves checking the user's credentials (username and password) and the process of granting access rights include establishing limits on that access. Auditing is the process of looking at past data to see whether there have been security breaches [14]. Intelligence systems for cloud security should adhere to auditing protocols, capture audit data in audit log files, and use a continuous monitoring system [15]. The cloud administrator should authenticate the user as a safe technique for first password distribution. Identifying, Confidentiality, Authorization, Accounting, Authentication, Auditing, and Privacy are some important principles used in cloud storage security and maintenance. The determination of authorization levels follows the establishment of user identity and authentication. [16].

III. SECURITY ASSERTION MARKUP LANGUAGE (SAML)

The OASIS SAML is a language that may be used to send authentication and authorization messages that are based on XML. The information that an asserting party asserts to be true about a principal is carried in SAML assertions by way of XML assertions. Authentication Assertion, Attribute Assertion, Decision Assertion, and Authorization Assertion are only a few of the many security assertions defined by SAML. The SAML identity federation technique allows for the connection of accounts across different sites while yet protecting user privacy. Pseudonyms are used. Users' identities across other sites will be connected via the use of pseudonyms provided by Identity Provider. Pseudonyms, together with digital signatures that verify the messages' origin,

International Journal of Core Engineering & Management
Volume-6, Issue-12, 2021 ISSN No: 2348-9510

will allow users to communicate across sites. The SAML protocol's process is shown in figure 3[17].

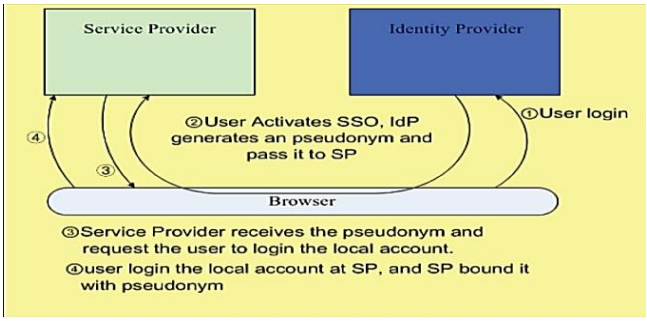

Fig. 3. The workflow of SAML protocol

The Figure 3 illustrates the workflow of the SAML protocol, which is a standard for web-based single sign-on (SSO). Here's a breakdown of the steps involved:

- **User login:** This user is trying to connect to a service that is offered by an SP.
- **User Activates SSO, IdP generates a pseudonym and pass it to SP**: For authentication purposes, the SP reroutes the user to the Identity Provider (IdP). A distinct pseudonym is created for the user by the IdP and sent to the SP.
- **Service Provider receives the pseudonym and request the user to login the local account:** The SP receives the pseudonym and prompts the user to log in to their local account.
- **User login the local account at SP, and SP bound it with pseudonym**: The user logs in to their local account at the SP, which then associates the user's local account with the pseudonym.

3.1 SAML For Multifactor Cloud Authentication

SAML provides a secure, XML-based framework for identity providers (like our organization) and service providers to share user security information. The SAML standard defines data exchange rules and syntax and allows external service providers to receive custom data. SAML transactions involve an asserting party, a relying party, and a subject [18]. User information is provided by the claiming party, or identity provider. The data provided by the claiming party is trusted by the service provider, who then utilises it to propose an application to the user. Transaction subjects are individuals and their identities [19]. SAML standard components are assertions, protocols, bindings, and profiles. Companies can customize standard layers for specific business applications. SAML assertions involve asserting and dependent parties. Relying parties trust all asserting party data. The XML schema-based SAML assertion structure includes headers, topic statements, attributes, and conditions. The assertion might include authorization declarations to grant web application user permissions. Service and identity providers exchange assertions using SAML request and answer protocols [20]. Figure 3 shows the Identity Provider Initiated SAML Assertion Flowchart.

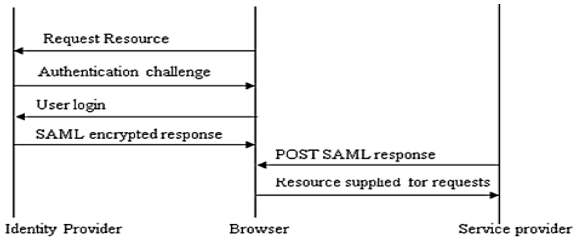

Fig. 4. Identity Provider Initiated SAML Assertion Flowchart

International Journal of Core Engineering & Management
Volume-6, Issue-12, 2021 ISSN No: 2348-9510

The Figure 4 provided illustrates the Identity Provider Initiated SAML Assertion Flowchart. This flowchart outlines a step involved in a SAML authentication process where the Identity Provider (IdP) initiates the authentication request. Here's a breakdown of the steps depicted in the diagram:

- **Request Resource:** The user, represented by the Browser, requests access to a resource from the SP.
- **Authentication Challenge:** An SP, unable to verify the user's identity, sends an authentication challenge to an IDP.
- **User Login:** The IdP prompts the user to log in using their credentials.
- **SAML Encrypted Response**: The user's identity details are included in a SAML assertion that is generated by the IdP when the login process is successful. This assertion is encrypted for security purposes.
- **POST SAML Response**: The IdP sends the encrypted SAML assertion to the SP using the HTTP POST method.
- **Resource Supplied for Requests**: Making reference to the SAML framework, the SP gets the SAML assertion and after ascertaining the validity of the assertion, admits an user to the requested resource.

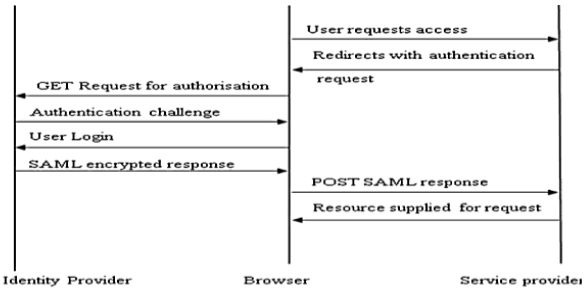

Fig. 5. Service Provider Initiated SAML Assertion Flowchart

The Figure 5 provided illustrates the Service Provider Initiated SAML Assertion Flowchart. The following describes how the SP is able to request a user's identity and his/her identity is authenticated by the IdP. Here's a breakdown of the steps involved:

- **User Requests Access**: The process starts when the user visits the SP's web site and asks to be granted access to a protected resource.
- **Redirects with Authentication:** The server of the public part directs the user to the web page of the identity provider for the purpose of authentication.
- **GET Request for Authorization**: An authorization request is sent by the identity provider to the SP in the form of a GET request.
- **Authentication Challenge**: The service provider issues an authentication challenge to the user, more often inquiring from the user his/her login details (user name and password).
- **User Login**: The user enters their credentials and logs in to the identity provider.
- **SAML Encrypted Response**: A SAML assertion is created by the identity provider, which includes the user's details and is encrypted with a shared secret with the SP.
- **POST SAML Response**: The identity provider uses a POST request to return the SP the encrypted SAML assertion.
- **Resource Supplied for Request**: This resource is made available to the user once the SP decrypts the SAML assertion and confirms its validity.

International Journal of Core Engineering & Management
Volume-6, Issue-12, 2021 ISSN No: 2348-9510

IV. LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)

ITU and ISO released X-500, a directory service standard, in 1990. The key feature of X-500 is a global distributed system that provides directory-wide access. DAP is utilized by clients to access directories in X-500. Data search hierarchy could be simplified by X-500. For desktops, X-500 service protocol was too hefty. In 1993, a scholar from Michigan University and ISODE Consortium developed a TCP/IP protocol. The outcome is LDAP. TCP/IP client-server protocol LDAP accesses and manages directory data. The solution's integrated directory services and user information storage fulfil the requirements of high security, single sign-on, and centralised user administration. Users can simultaneously access applications, services, and servers and choose their privileges. This protocol allows access to the X-500 directory without the essential resources for LDAP implementation [21].

4.1 LDAP Working System

A client-server approach underpins LDAP's operation, which is comparable to that of X.500. Similarly, to the procedure in X.500, the client query process is unique. To make a query, the client will submit an identifier, which will accept the characteristics. When a client sends a query packet via TCP/IP, the LDAP server uses the DIT (Directory Information Tree) to find the corresponding identification. As soon as it is located, the client's computer will get the result immediately. However, in the event that the requested information cannot be located, the client will get a reference to another LDAP server. The figure 6 shows the working mechanism of LDAP.

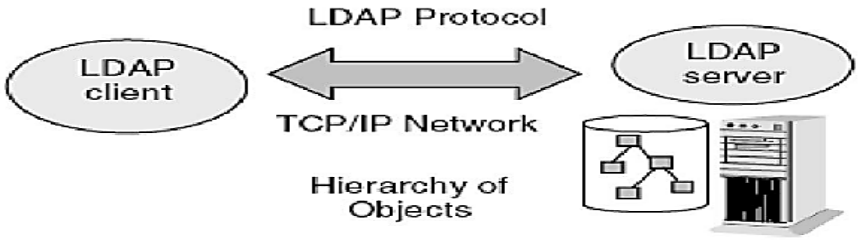

Fig. 6. Working Mechanism of LDAP

V. LDAP Cloud Authentication

A few benefits of LDAP authentication are a condensed user account count, streamlined user and permission administration, and centralised storing of user information. The figure 7 depicts the LDAP authentication scheme [22].

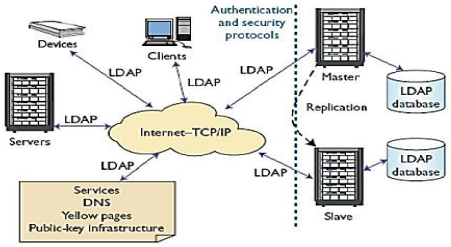

Fig. 7. LDAP Authentication Scheme

Today, organizations, including universities and SMEs, must offer diverse services to numerous users in computing. Many services require authentication or authorization to validate subscriber

International Journal of Core Engineering & Management
Volume-6, Issue-12, 2021 ISSN No: 2348-9510

identities securely. Authentication may be necessary for remote terminal clients like SSH and email clients like Zimbra. An organization's productivity and financial profits may be hampered by a denial-of-service assault on a hacked LDAP server.

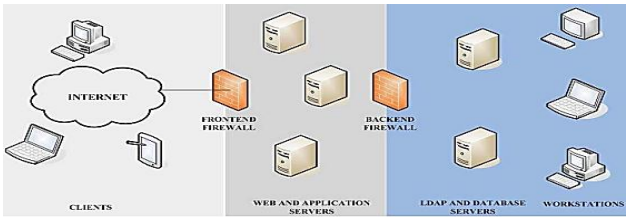

Fig. 8. Standard enterprise network configuration

The figure 8 below shows the standard enterprise network configuration. Firewalls and IDS are common ways that important LDAP servers in business contexts are protected. Security policies are often compromised due to LDAP being an active directory, resulting in IT departments opening servers to the Internet. Although firewalls are effective, well-crafted TCP SYN packets can still create SYN flooding symptoms [23].

VI. SAML AND LDAP USE CASES FOR CLOUD-BASED ENTERPRISE AUTHENTICATION AND AUTHORIZATION

Both SAML and LDAP play crucial roles in cloud-based enterprise authentication and authorization, catering to different needs. SAML is appropriate for cases of SSO across several cloud applications and for the improvement of usability in mobile and partnership contexts. On the other hand, LDAP caters organizations with on-premises and hybrid solutions, especially organizations requiring efficient user management, as well as organizations with existing infrastructure. Combined, the technologies in this article can form a cocktail of methods of identification in the cloud which considers usability and adds an extra layer of protection.

6.1 SAML Use Cases

Here's a concise overview of SAML use cases for cloud-based enterprise authentication and authorization:

A. Cloud-Based Applications

Certainly, SAML is most valuable for organizations that employ several cloud applications, for instance, Salesforce, Google Workspace, or Microsoft 365. It is a single sign-on authentication method thus reducing the complexity of log in for users across the different interfaces. An organization can employ SSO through SAML to mean that a user will only sign in once to be granted access to other apps that are trusted. This increases the usability of the applications and minimizes the problem of password exhaustion [24].

B. Enterprise Mobility

There ought to be as much application access for remote workers as there would be for those in an office. This is because SAML makes the use of a common authentication scheme possible. Employees and partners can quickly work with business applications from various devices, staying efficient and secure at the same time. SAML has been used to enforce a security policy while at the same time allowing the users outside the organization to sign in easily [25].

International Journal of Core Engineering & Management
Volume-6, Issue-12, 2021 ISSN No: 2348-9510

C. *Partnerships*

For organizations engaged in B2B partnerships, SAML allows external partners to access specific applications without requiring them to create and manage separate accounts within the internal directory. This simplifies collaboration, as partners can use their existing credentials from their own identity providers to access the necessary resources, streamlining the authentication process while maintaining security [26].

VII. LDAP Use Cases

Here's a concise overview of LDAP use cases for cloud-based enterprise authentication and authorization:

A. *On-Premises and Hybrid Solutions*

LDAP is great for certain deployment, especially when an enterprise has number of applications on the local network or has a hybrid cloud infrastructure. It also works as a user directory; users can be managed within this directory and their attributes too. Administrators can retain control of the user identity and their sign-on process thus allowing it to be easily deployed within existing infrastructures and provide secure aperture to both on PREM and cloud based applications [27].

B. *User Management in Large Enterprises*

Most big organizations have a lot of users who need to be governed by attributes, roles and privileges. In this area LDAP proves to be one of the best because it offers a structure solution for user information. LDAP allows an organization to manage users from creation to modification to deletion, with an effective control of rights to access information [28].

C. *Integration with Legacy Systems*

There are several organizations that continue to implement old structures that mandate LDAP for authorization. Summarizing, such systems' integration with the modern application may be problematic in the absence of the suitable directory service. This is made possible by LDAP where it can act as an authentication layer, enabling legacy systems to communicate with modern applications, retain user management tradition they have embraced [29].

Here's a comparison table 1 outlining the best practices and use cases for SAML and LDAP in cloud-based enterprise authentication and authorization:

TABLE I. SAML VS LDAP

Feature	SAML	LDAP
Overview	Open standard for exchanging authentication and authorization data.	Protocol for accessing and managing directory information services.
Primary Use	Enables Single Sign-On (SSO) for cloud applications.	Manages user authentication and information retrieval in internal systems.
Best Practices	• Implement SSO for improved user experience. • Utilize strong security measures (signed and encrypted assertions). • Leverage identity federation with	• Centralize user management for consistency. • Enforce strong password policies. • Implement access control with ACLs.

	external IdPs. • Monitor and audit access regularly. • Periodically review configurations for compatibility.	• Use LDAPS for secure communication. • Regularly back up directory data and have a recovery plan.
Use Case: Cloud-Based Applications	Ideal for organizations using multiple cloud services (e.g., Salesforce, Google Workspace).	Not primarily focused on cloud applications; more suited for internal systems.
Use Case: Enterprise Mobility	Provides seamless access for mobile and remote workforces.	Primarily supports internal user management rather than mobility.
Use Case: Partnerships	Effective for B2B collaborations allowing external partners to authenticate.	Not typically used for external partnerships; focuses on internal directory access.
Use Case: On-Premises Solutions	Less applicable for on-premises solutions; focuses on cloud environments.	Best suited for organizations with hybrid environments or on-premises applications.
Use Case: User Management	Limited user management capabilities; focuses on authentication.	Excels in managing large user bases, attributes, roles, and permissions.
Use Case: Integration with Legacy Systems	Not designed for legacy system integration.	Effective for integrating legacy applications that rely on LDAP for authentication.

VIII. LITERATURE REVIEW

This section encapsulates the literature review available on SAML and LDAP for best practices for cloud-based enterprise authentication and authorization. The table II below shows the summary of the literature review.

This study Hamza, Abubakar and Danlami, (2018) identifies the primary computational challenge as the administration of enterprise user and application digital identities and access control. They used LDAP for authentication, authorization, identity administration, and audit reporting with IAM-Sys. It focusses on cloud or on-premises entity verification and resource access. The research employed a staged strategy, which requires careful planning and technology knowledge. Participants' average rating score was 72.0% in the experiment. If properly configured, IAM-Sys can alleviate authentication, authorization, data protection, and accountability security risks [30].

In this paper Qadeer, Salim and Sana Akhtar, (2009), They demonstrate how to utilise LDAP to control user profiles and authentication. The LDAP-DIT holds user profiles that include several pieces of information about individuals. Users' ability to access this data is proportional to the permissions granted to them online. A number of services rely on this authentication technique to provide access to authorised users who supply the necessary authentication details contained in the LDAP data. A variety of server applications may make use of LDAP for user authentication, including VPNs, RAS, web servers, and mail servers [31].

In this paper Sari and Hidayat, (2006), They narrate the story of how they used the LDAP authentication technique to get user IDs from an LDAP server in order to secure our HR information system web server application. secure, centralised user administration, and single sign-on are all requirements of LDAP. With this protocol, you may store and manage user

information in a directory while also taking use of security services. As a result, the user may simultaneously set permissions, applications, and services [32].

This paper Lewis, (2009), discusses the capabilities and implementation of SAML to provide secure single sign-on (SSO) solutions for apps hosted elsewhere. Businesses are increasingly relying on web-based services provided by ASPs or SaaS suppliers to provide targeted applications to customers at a reduced cost. An enormous boon to organizations is that this technique removes the complexity of system design, installation, configuration, deployment, and support via the use of internal resources [33].

This paper Obimbo and Ferriman, (2011a), investigates the potential risks of using LDAP for user authentication by conducting a DoS attack that takes advantage of the TCP three-way handshake that is necessary to establish a connection to an LDAP server. The authentication of users in enterprise-level networks is facilitated by (LDAP) servers. Education institutions and SMEs rely on LDAP for a range of services, including authentication for workstations, secure shell, and electronic mail clients. Since several organizations rely on the LDAP service, a DoS attack on the service may impair a higher number of services [34].

In this paper Indu, Rubesh Anand and Bhaskar, (2017) that cloud web services may now benefit from customised SAML technology, which enables token-based fine-grained authentication. Encryption is used to increase the security of all communications between the Identity Provider, the Service Provider, and the Cloud Server. Cloud web services are more secure when SAML and verification based on single use access tokens are used together. By allowing for the addition of an unlimited number of trustworthy sources and web services, the suggested modified SAML authentication technique guarantees an environment that is both flexible and scalable [24].

TABLE II. SUMMARY OF RELATED WORKS FOR SAML AND LDAP FOR CLOUD-BASED ENTERPRISE AUTHENTICATION AND AUTHORIZATION

Ref.	Topic	Approach	Findings	Significance	Challenges	Future Work
[30]	Enterprise Identity Management	Utilized LDAP for authentication and access control	Average participant rating: 72.0%.	IAM-Sys mitigates security risks when properly configured.	Complexity in integration with existing systems.	Explore integration with emerging identity protocols.
[31]	User Profile Management	Managed user profiles in LDAP Directory Information	Authorized users can access services with correct credentials.	LDAP facilitates service access based on user authentication.	Ensuring data consistency and accuracy in profiles.	Investigate user experience improvements in access management.

		Tree				
[32]	HR System Authentication	Implemented LDAP for HR web server application	Enhanced centralized user management and security.	Provides a single sign-on and secure user data management.	High security demands and user privacy concerns.	Develop more advanced encryption techniques for user data.
[33]	Secure Single Sign-On	Implemented SAML for external application authentication	Simplified deployment and support for SSO solutions.	Reduces complexity for organizations using external services.	Integration challenges with various service providers.	Research scalable SSO solutions for diverse environments.
[34]	LDAP Vulnerabilities	Analyzed DoS attacks on LDAP servers	LDAP service disruptions can affect multiple applications.	Highlights risks associated with LDAP in enterprise networks.	Increasing sophistication of attack methods.	Develop robust countermeasures against DoS attacks on LDAP.
[24]	Fine-Grained Cloud Authentication	Proposed SAML with token-based security for cloud services	Improved security through encrypted communication.	Supports scalability with multiple trusted sources.	Complexity in managing token lifecycle and expiration.	Explore enhanced token management strategies and protocols.

IX. CONCLUSION AND FUTURE WORK

SAML and LDAP are two separate components of business identity management that work together. It also functions well in the context of clouds where SSO and federated identity are the most crucial components, using token-based authentication to grant convenient access to many applications. This is specifically because SAML works well with web services-based platforms and the cloud which makes it one of the best for organizations that are migrating to the cloud. However, LDAP is great at handling directory-based authentication, as well as access control in more conventional, on-premises settings. A feature of mine is a strong hierarchical directories array and organizations with vast levels of legacy infrastructure are well served by its incorporation. SAML and LDAP should be chosen according to the specific tendencies – how the business is going to use it, what level of security is required, and how the system should scale. This review also supports the efforts to understand the limitations and advantages of each protocol indicating that in some cases the best approach would be to try and combine the two technologies. By ensuring that updates are provided frequently, and with correct encryption, and by adhering to best practices where security is concerned, the implementation of these protocols in defence of enterprise networks will go a long way in ensuring their effectiveness.

REFERENCES

1. M. Ramachandran and V. Chang, "Towards performance evaluation of cloud service providers for cloud data security," Int. J. Inf. Manage., 2016, doi: 10.1016/j.ijinfomgt.2016.03.005.
2. D. M. Mangiuc, "Cloud Identity and Access Management – a Model Proposal.," Account. Manag. Inf. Syst. / Contab. si Inform. Gestiune, 2012.
3. M. Alizadeh, S. Abolfazli, M. Zamani, S. Baaaharun, and K. Sakurai, "Authentication in mobile

cloud computing: A survey," Journal of Network and Computer Applications. 2016. doi: 10.1016/j.jnca.2015.10.005.
4. S. Y. Lim, M. L. Mat Kiah, and T. F. Ang, "Security issues and future challenges of cloud service authentication," Acta Polytech. Hungarica, 2017, doi: 10.12700/APH.14.2.2017.2.4.
5. V. V Kumar, M. Tripathi, M. K. Pandey, and M. K. Tiwari, "Physical programming and conjoint analysis-based redundancy allocation in multistate systems: A Taguchi embedded algorithm selection and control (TAS&C) approach," Proc. Inst. Mech. Eng. Part O J. Risk Reliab., vol. 223, no. 3, pp. 215–232, Sep. 2009, doi: 10.1243/1748006XJRR210.
6. I. R. Chen, B. Gu, S. E. George, and S. T. Cheng, "On failure recoverability of client-server applications in mobile wireless environments," IEEE Trans. Reliab., 2005, doi: 10.1109/TR.2004.837518.
7. Z. Wang, N. Wang, X. Su, and S. Ge, "An empirical study on business analytics affordances enhancing the management of cloud computing data security," Int. J. Inf. Manage., 2020, doi: 10.1016/j.ijinfomgt.2019.09.002.
8. B. Rashidi, "Authentication issues for cloud applications," 2019, pp. 209–240. doi: 10.1049/PBSE009E_ch9.
9. B. P. Rimal, E. Choi, and I. Lumb, "A taxonomy and survey of cloud computing systems," in NCM 2009 - 5th International Joint Conference on INC, IMS, and IDC, 2009. doi: 10.1109/NCM.2009.218.
10. D. J. Abadi, "Data Management in the Cloud : Limitations and Opportunities," Bull. IEEE Comput. Soc. Tech. Commitee Data Eng., 2009.
11. R. Goyal, "The Role Of Business Analysts In Information Management Projects," Int. J. Core Eng. Manag., vol. 6, no. 9, pp. 76–86, 2020.
12. M. A. Shibli, R. Masood, U. Habiba, A. Kanwal, Y. Ghazi, and R. Mumtaz, Access Control As a Service in Cloud: Challenges, Impact and Strategies, no. July. 2014. doi: 10.1007/978-1-4471-6452-4_3.
13. U. Khalid, A. Ghafoor, M. Irum, and M. A. Shibli, "Cloud based secure and privacy enhanced authentication & authorization protocol," in Procedia Computer Science, 2013. doi: 10.1016/j.procs.2013.09.149.
14. V. V. Kumar and F. T. S. Chan, "A superiority search and optimisation algorithm to solve RFID and an environmental factor embedded closed loop logistics model," Int. J. Prod. Res., 2011, doi: 10.1080/00207543.2010.503201.
15. V. V. Kumar, M. K. Pandey, M. K. Tiwari, and D. Ben-Arieh, "Simultaneous optimization of parts and operations sequences in SSMS: A chaos embedded Taguchi particle swarm optimization approach," J. Intell. Manuf., 2010, doi: 10.1007/s10845-008-0175-4.
16. J. Vijaya Chandra, N. Challa, and S. K. Pasupuletti, "Authentication and authorization mechanism for cloud security," Int. J. Eng. Adv. Technol., 2019, doi: 10.35940/ijeat.F8473.088619.
17. W. L. C. L. P. Chu, "SAML-Based Access Control with Location Attributes System SAML-Based Access Control with Location Attributes System," no. May, 2013, doi: 10.13140/2.1.1423.4887.
18. V. K. Y. Mohamed Ali Shajahan, Nicholas Richardson, Niravkumar Dhameliya, Bhavik Patel, Sunil Kumar Reddy Anumandla, "AUTOSAR Classic vs. AUTOSAR Adaptive: A Comparative Analysis in Stack Development," Eng. Int., vol. 7, no. 2, pp. 161–178, 2019.
19. V. V Kumar, M. Tripathi, S. K. Tyagi, S. K. Shukla, and M. K. Tiwari, "An integrated real time optimization approach (IRTO) for physical programming based redundancy allocation

problem," Proc. 3rd Int. Conf. Reliab. Saf. …, no. August, 2007.
20. B. Prasanalakshmi and A. Kannammal, "Secure Credential Federation for Hybrid Cloud Environment with SAML Enabled Multifactor Authentication using Biometrics," Int. J. Comput. Appl., 2012, doi: 10.5120/8520-2328.
21. B. P. Vamsi Krishna Yarlagadda, Sai Sirisha Maddula, Dipakkumar Kanubhai Sachani, Kishore Mullangi, Sunil Kumar Reddy Anumandla, "Unlocking Business Insights with XBRL: Leveraging Digital Tools for Financial Transparency and Efficiency," Asian Account. Audit. Adv., vol. 11, no. 1, pp. 101–116, 2020.
22. V. Koutsonikola and A. Vakali, "LDAP: Framework, practices, and trends," IEEE Internet Comput., 2004, doi: 10.1109/MIC.2004.44.
23. J. Maria ALONSO, A. GUZMAN, M. BELTRAN, and R. BORDON, "LDAP Injection Techniques," Wirel. Sens. Netw., 2009, doi: 10.4236/wsn.2009.14030.
24. I. Indu, P. M. Rubesh Anand, and V. Bhaskar, "Encrypted token based authentication with adapted SAML technology for cloud web services," Journal of Network and Computer Applications. 2017. doi: 10.1016/j.jnca.2017.10.001.
25. Y. Wang, Y. Chen, T. Zhu, and D. Lin, "Unpacking the organizational impacts of enterprise mobility using the repertory grid technique," Internet Res., 2018, doi: 10.1108/IntR-10-2016-0293.
26. K. Money, C. Hillenbrand, M. Day, and G. M. Magnan, "Exploring reputation of B2B partnerships: Extending the study of reputation from the perception of single firms to the perception of inter-firm partnerships," Ind. Mark. Manag., 2010, doi: 10.1016/j.indmarman.2010.02.015.
27. F. Trovato, A. Sharp, and T. Siman, "Cloud, co-location, on-premises and hybrid disaster recovery solutions: Pros, cons, and a cost comparison," J. Bus. Contin. Emer. Plan., 2019, doi: 10.69554/xzaa5492.
28. G. N. Priya, A. K. Sangaiah, A. Thangavelu, T. Murali, and B. Balusamy, "Providing efficient user management for large-scale enterprise by achieving high scalability over cloud," Int. J. Internet Protoc. Technol., 2017, doi: 10.1504/IJIPT.2017.087545.
29. M. W. M. W. M. W. Chowdhury and M. Z. M. Z. Iqbal, "Integration of Legacy Systems in Software Architecture," SAVCBS 2004 Specif. Verif. ComponentBased Syst., 2004.
30. M. K. Hamza, H. Abubakar, and Y. M. Danlami, "Identity and Access Management System: a Web-Based Approach for an Enterprise," Path Sci., vol. 4, no. 11, pp. 2001–2011, 2018, doi: 10.22178/pos.40-1.
31. M. A. Qadeer, M. Salim, and M. Sana Akhtar, "Profile management and authentication using LDAP," in Proceedings - 2009 International Conference on Computer Engineering and Technology, ICCET 2009, 2009. doi: 10.1109/ICCET.2009.126.
32. R. F. Sari and S. Hidayat, "Integrating web server applications with LDAP authentication: Case study on human resources information system of UI," 2006 Int. Symp. Commun. Inf. Technol. Isc., no. March, pp. 307–312, 2006, doi: 10.1109/ISCIT.2006.340053.
33. K. D. L. andjames E. Lewis, "Web Single Sign-On Authentication using SAML," no. June, 2009, doi: 10.48550/arXiv.0909.2368.
34. C. Obimbo and B. Ferriman, "Vulnerabilities of LDAP As An Authentication Service," J. Inf. Secur., 2011, doi: 10.4236/jis.2011.24015.