International Journal of Applied Mathematics

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

AN ANALYSIS OF AUTHENTICATION MODELS IN IDENTITY MANAGEMENT SYSTEMS, INCLUDING KERBEROS, AD, AZURE AD, OPEN AD, OPENLDAP, AND DATABASES

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

[1]Research Scholar, PG & Research, Department of Computer Science, Government Arts college (Autonomous), karur, Affiliated to Bharathidasan University, Tamil Nadu, India, raja@inflibnet.ac.in

[2]Associate Professor, PG & Research, Department of Computer Science, Government Arts college (Autonomous),), karur, Affiliated to Bharathidasan University, Tamil Nadu, India, Tamil Nadu, India, banukarthikeyan7811@gmail.com

[3]Professor, Department of Computer Science and Engineering, Unitedworld Institute of Technology, Karnavati University, Gujarat, India, manivelk79@gmail.com

Abstract

This research discusses the different types of authentication models used in identity management systems. Some models specifically mentioned are Kerberos, Active Directory (AD), Azure Active Directory (Azure AD), Open Active Directory (Open AD), and OpenLDAP. The identity management system is the security framework that manages the digital identity verifying authentication to determine the level of access to have specific resources followed by verified identity. The Need for IMS to ensure authorized individual access to organizational resources. While assessing each model's scalability, security features, and performance in various organizational environments, the study also looks at its use cases, shortcomings, and strengths. Kerberos is the network authentication protocol, that provides secure authentication through user services in client-server architecture. Validate identity to ensure about exchange of the relationship between the user and services. Advantages as strong security and time-based authentication. Azure Active Directory is a cloud-based solution, that helps businesses secure and manage to access the various ranges of on-premises and cloud-based app services. The advantage of this is to identify the security and protection with MFA and SSO. Open AD provides the directory service and identity management. The authentication process is similar to the traditional active directory with flexibility and transparency among the open-source software. Open LDAP is used to manage the directory services to handle the authentication process in network environments. Database authentication helps to verify and identify the database to store and retrieve the authentication credentials. Compared with existing models, these are all integrated with Windows applications. The authentication models provide security, flexibility, scalability, and cost-effective solutions.

Key Words and Phrases: Authentication models, Identity management systems, kerberos, active directory, azure AD, open AD, OpenLDAP, Database authentication,

Received:August 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Security, scalability, Multi-factor authentication (MFA), Federated identity, Cloud-based identity management.

1. Introduction

The term "authentication models" in Identity Management Systems (IMS) refers to the techniques used to confirm a user's identity when accessing a system. These techniques typically include password-based authentication, multi-factor authentication (MFA), biometric authentication, token-based authentication, and certificate-based authentication. The aim is to guarantee that only authorized users have access to sensitive data and systems; important components include identity federation, strong password policies, and role-based access control (RBAC) to manage user restrictions efficiently. Key authentication models included password-based authentication, Biometric authentication, Identity Federation, strong password policies, adaptive authentication, and security [1] [2].

Cloud services are used by the two types of authentication methods such as digital security and physical security. Physical security also measured as fingerprint recognition, depends upon biometric authentications. Digital security measures are also related to factor authentication, which is the most popular technique for cloud computing access through management, password credentials, and SSO. To overcome this issue, various types of security standards are used. Include access control over the governance and mechanisms. It is the most effective way to analyze the security of cloud services to identify access management. The framework contains two-factor authentication it’s also enhanced to verify the user access to analyze the private cloud services. The Open stack tool is used for analysis of the framework and sends the secret QR code to every user. Another way to raise the authentication level in cloud computing use biometric, graphical passwords. To maintain the security of cloud computing services and authentication techniques are have adaptable with effectiveness. It is a difficult task to build the cloud authentication framework to maintain the identity for access management with high flexibility and efficiency.

In the modern area, secured to access the system and resources are related to organizations. Followed by Authentication, which is the process of verifying the identity of a user or system. An effective identity management system should ensure that individuals access the data and services while preventing unauthorized access. From the analysis, different types of authentication models and protocols are used to identify the management system. Some key technologies are Kerberos, Active Directory, Azure AD, Open Ad, Open LDAP and database [3] [4]. Kerberos is the authentication protocol that employs symmetric ley cryptography enable to secure authentication across the network [5][6]. Active Directory is commonly used for managing identities and resources related to corporate networks. Open AD is a cost-effective solution for identity management. Most organizations use databases to store user credentials, which are managed to access the control used by various mechanisms such as SQL-based authentication and token-based authentications.

Received:August 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2. Literature Review

The authorization and authentication procedures form the foundation of the IAM system. While the authorization process is based on granting or denying cloud resources based on user authorities, the authentication process is used to make sure that end users are legitimate. IAM's overall evaluation was suggested using a different assessment. According to the proposed work, to guarantee the effectiveness of IAM, various identity management features must be offered. Several cloud-based identity management system techniques are explained and examined. The authors conducted a comparative analysis, outlining the pros and cons of each authentication method Luu et al., [16]. It was discussed how to manage identity in a hybrid cloud.

Recent identity and access management (IAM) security models, their security architectures, and security concerns are the main topics of the remaining related works. Models of IAM Services to assess the privacy of stored data, storage services, and identity and access management performance-based data storage, various IAM service models have been implemented and suggested. It is suggested to store user identities in cloud computing data. File management is done via identity-based proxy re-encryption. There are numerous disadvantages when access to data is granted by the central authority. Additionally, the suggested schemes are vulnerable to certain kinds of closure attacks. To ensure the integrity of user profiles, several techniques are used, depending on the data that is stored on the cloud. In recent years, a lot of businesses have moved their services to cloud platforms. Using the cloud for storage raises concerns about user privacy control Chandra et al., [20]. The conventional approach, which relies on privacy controls like username and password, is unable to shield users from phishing, sniffing, and virtualization attacks. From the below table, 1 describes a comparison of the various authentication protocols implemented by different researchers. This table shows the advantages and limitations of existing protocols.

Table 1. Comparison of Existing Authentication Protocol

Reference Number	Protocol Implementation	Advantages	Disadvantages
[13]	SMAP	Short authentication delay for network handling.	Results as false positive followed by BAN logic.
[11]	EAP GPSK	Flexible Lightweight usage of symmetric cryptography.	DoS attack- followed by non-standard derivations.
[12]	Micro Certificate Authentication	High Speed-fast security	Deployment is higher.

Received:August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[10]	SWAP	Unique OTP-protect passwords	SMS Delay-performance Eavesdropping.
[9]	EAP Re-Authentication Protocol	Low CPU Usage	Complex key management.
[8]	Hybrid Security Protocol	Short response time	Both types of cryptography are used.

Author Baqer et al., [10] SMAPs, or short message authentication protocols, are an offline payment protocol that was suggested for places with erratic or nonexistent network connectivity. It was created with less developed nations in mind. It made offline transactions more usable by minimizing the number of digits a user must hear, speak, and type. It also ensured that there were no scalable attacks big enough to be a concern and offered strong recovery mechanisms for the inevitable errors. Additionally, the protocol can make delay-tolerant authentication possible for payment networks. Mitchell et al [11] created the pre-shared key and symmetric cryptography-based EAP-GPSK, a lightweight and adaptable authentication protocol. The IETF EAP Method Update (EMU) working group was responsible for its development. The protocol decreased the number of round trips and works well with devices with low memory and processing power. They found errors using a finite-state model, and after fixing the errors, they proved correctness using Protocol Composition Logic. Furthermore, it permits the negotiation of cryptographic cipher suites that specify the key derivation algorithm, message integrity mechanism, and encryption algorithm (if any) that the protocol participants will employ. LiPing Du et al [12] introduced an authentication protocol based on micro-certificates that is lightweight and applicable to both the Internet and the Internet of Things. This authentication mechanism stores the crucial secret information on a CPU security chip and creates a micro-certificate for the authentication protocol using fewer authentication parameters. The use of micro certificates, which are dynamic, improves security. To accomplish the authentication, symmetric cryptographic algorithms, CSK technology, a cipher chip technology were employed. Its advantages over other authentication protocols include its small size, high security, and speed. Rajesh et al., [13] suggested a user authentication protocol based on OTP, which offers defense against password reuse, theft, and collision attacks. Compared to traditional web authentication methods, SWAP (Secure Web Authentication Protocol) is more cost-effective and efficient. Eliminating the detrimental effects of the human factor is the design principle. Each participating website only needs to have a distinct phone number, and there are registration and recovery phases.

3. Authentication Model Analysis

3.1. Kerberos Architecture & Implementation

Received:August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Authentication over an open network can be dependable with the Kerberos authentication protocol fig:1, It offers an authentication system that allows both clients and servers, or two distinct servers, to authenticate each other [14]. Instead of using passwords to access the network, the Kerberos protocol uses specially formatted data packets called tickets [7]. Encryption keys are used to make sure that no one can alter the client's ticket or any other data contained in a Kerberos message. The Kerberos authentication procedure works as follows: The authentication server (AS) receives a request from the client for the server's "credentials." The result is a client-specific coded key. Credentials include a temporary encryption key (also known as a "session key") and a "ticket" for the server. The ticket is transmitted to the server by the client. The client and server can both be authenticated using the session key, which is optional.

The authorization model is founded on the idea that each service can maintain its authorization information since it knows the user. The Kerberos Authentication System can be extended with data and authorization-related algorithms. Implementing the protocol necessitates one or more hosts. The authentication servers keep the secret keys and principals in a database. Code libraries carry out the Kerberos protocol and offer encryption [23]. The Generic Security Services Application Programming Interface or the Kerberos library itself is called by a typical network application.

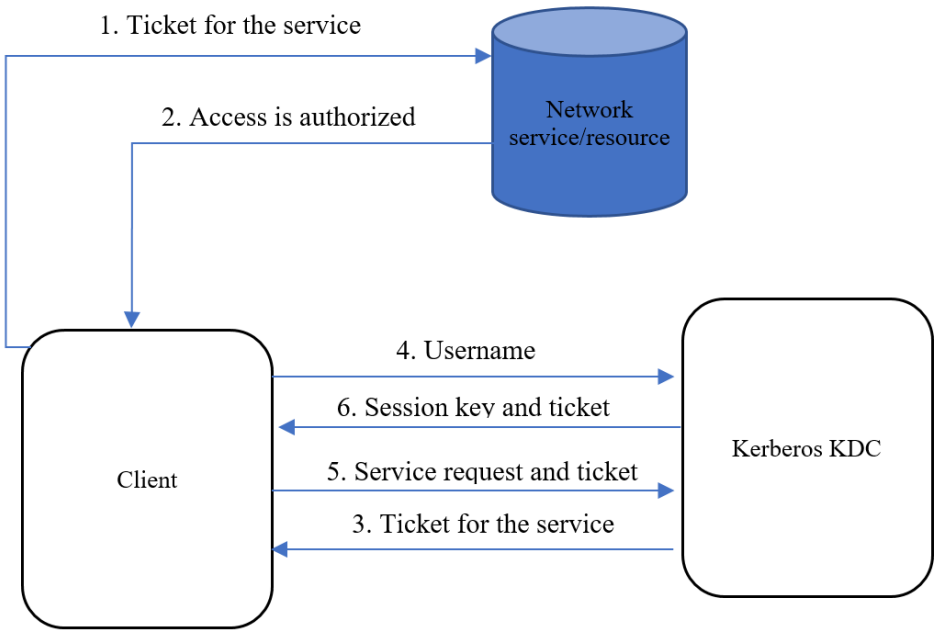

Fig.1 Kerberos Protocol

The steps for an authentication Process are as follows:

Step 1: The client must contact with authentication server to receive a ticket as the encryption key.

Received:August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Step 2: The client received a ticket-granting ticket for an encryption key, called as session Key. Uses for to unlock the communication between the client and server to authenticate the communication.
Step 3: Client requests service ticket to Kerberos server, client access the particular service and sends the ticket to TGS.
Step 4: Identify the client for the requested services.
Step 5: Access the resources many times when with desired ticket expires.
Step 6: Mutual authentication

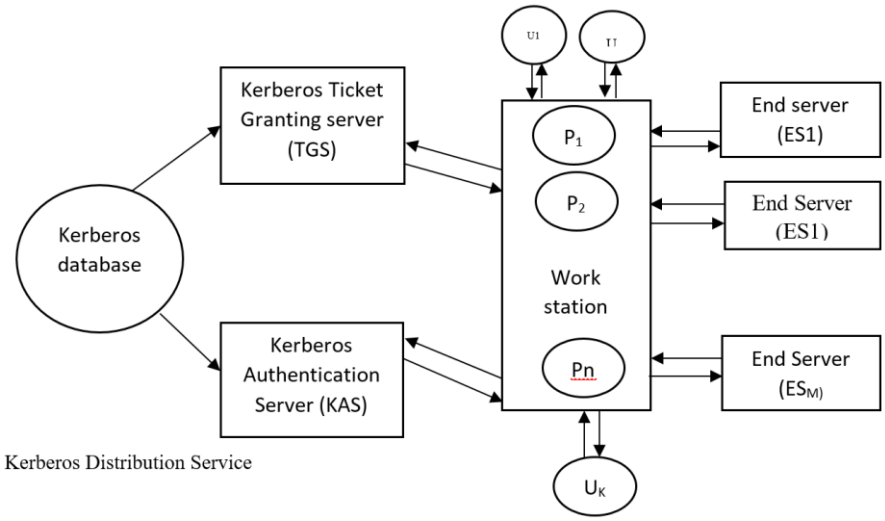

Fig. 2 Kerberos Authentication Architecture

The above fig 2 covers by Kerberos database, Kerberos Ticker Granting server, Authentication server, workstation, and End server. Authentication architecture consists of the following parties, workstation contains the set of a process as p1, ... pn, user noted as u1, ... uk the key set distribution service, which contains Es1, Es2, ... Esm. The Kerberos Key Distribution services turned into combining the two servers such as KAS and TGS. This model should keep the database with client and server keys. A client key is followed by DES coded version owned by the client. The main ideas of this model are followed by the use of services, the client must supply through the end server which provides a ticket obtained from Kerberos. The ticket for service encrypted is used by the server's private key. Based on this result, the client should be declared inside the ticket the server receives the ticker from Kerberos authenticated evidence among client identity.

3.1.1 Algorithm for Module Specifications

Authentification

KasReply rule of KAS_MODULE

Block

[check Identity rule]

Received:August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

If mode = Ready to Receive & KAS_Receive From_C:mssg & defined(K(c))

Then

Clear (mssg)

Mode : = Ready to Send

[Provide Authentication rule]

If mode = Ready to Send

Then

If defined (K(C,TGS)) & defined (Ticket (C, TGS))

Then

KAS_SendTo_C: {K (C,TGS), Ticket (C,TGS), TGS,CT} k ©

Mode: =Ready to Receive

Else

K (C, TGS): = Provide Key (C, TGS)

Ticket (C, TGS): = Provide Ticket (C, TGS)

End block;

Hence, C receives the KAS reply. If the test on the password succeeds and the message is considered recent, C extracts from the message the authentication key and the authentication ticket and saves its copies.

Get Authentication rule of C_MODULE_Authetication

If authenticated & mode = Ready to Receive

& C_ReceiveFrom_KAS: CryptedMssg

& Check Password (CryptedMssg, CodePsw ©))

& Check Valid (CryptedMssg, mark)

Then

K(C,TGS) : = Extract key (CryptedMssg)

Ticket (C, TGS):= Extract Ticket (CryptedMssg)

Clear (CryptedMssg)

Mode:= Ready To Send

End

3.2. Active Directory Authentication Model

Received:August 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

As cloud platforms and hybrid infrastructure models have become more prevalent, the identity management landscape has experienced a significant change. The intricate need to maintain stable, secure, and adaptable Active Directory (AD) environments that span both contemporary cloud ecosystems and conventional on-premises infrastructure is becoming a greater challenge for organizations. Given the dynamic nature of modern enterprise technology infrastructures, Active Directory deployment models have undergone significant evolution. Instead of limiting businesses, single-location directory services are now deploying advanced hybrid cloud scenarios that facilitate resource access and authentication in dispersed environments. Cloud-based Active Directory services are increasingly the go-to option for businesses looking to update their identity management procedures.

One of the most complex issues in hybrid cloud AD deployments is identity synchronization. For organizations to maintain uniform user profiles, attributes, and access permissions across a variety of technological environments, they must create strong strategies. Ensuring data consistency across various directory services, managing complex identity mappings, and handling real-time updates all require the use of advanced synchronization tools. In hybrid cloud AD deployments, identity synchronization is one of the trickiest problems. For organizations to maintain uniform user profiles, attributes, and access permissions across a variety of technological environments, they must create strong strategies. Table:2 Ensuring data consistency across various directory services, managing complex identity mappings, and handling real-time updates all require the use of advanced synchronization tools[17]. Fig:3 covers the authentication procedure as,

Table 2. Active Directory Authentication Model Assessment

Technological Aspect [13]	Complexity Level	Innovation Potential	Security Effectiveness
Federation Services [13]	High	85%	Robust
Authentication Mechanisms [13]	Moderate	90% Dynamic	Comprehensive
Trust Relationship Management [13]	Very High	88% Adaptive	Granular
Compliance Integration [13]	Complex	92% Intelligent	Strategic
Scalability Approach [13]	Challenging	95% Flexible	Transformative

3.2.1 Authentication Protocols

Received:August 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

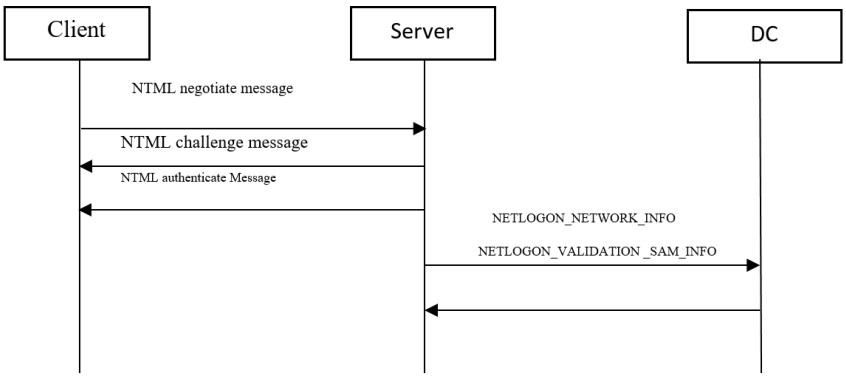

Fig. 3 Active Directory Authentication Model Authentication process

Procedures:

Step 1: Client Initiate the Authentication Request

Step 2: Authenticate the resource challenges provides a 16-bit random number

Step 3: Client combined with various challenges with hash and responds.

Step 4: Forward to the domain controller by resources

Step 5: Domain controller received a forward response against access status.

The benefit of AD only accesses the resources on the network ensures that authorized individuals have the entry of specific parts of the system. Its centralized user management consistent security policy enforcement across the network. Some key advantages of Active directory authentication are centralized authentication, single Sign, Group policy management, scalability, and enhanced security [18].

3.3 Azure Active Directory Authentication Model

Azure AD refers to verifying the identity of users or application access by the various resources. Its involved by to verifying the user credentials or other authentication methods to grant access. Examples of authentication models as username, password, MFA, and OAuth tokens. The key components of this authentication model as tokens and identity providers. The importance of this authentication model is to ensure legitimate users or application access through various resources.

Authentication in Azure AD is enhanced through security by allowing authorized users to access the organizational assets. To enable the users to access this authentication model effectively control the rights, secured through applications and services [19]. It's for to identify and verification should be required means to maintain the security measures to avoid unwanted access in Azure AD [24]. The authorization process in this model efficiently controlled access and enhanced the safety measures.

Received:August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

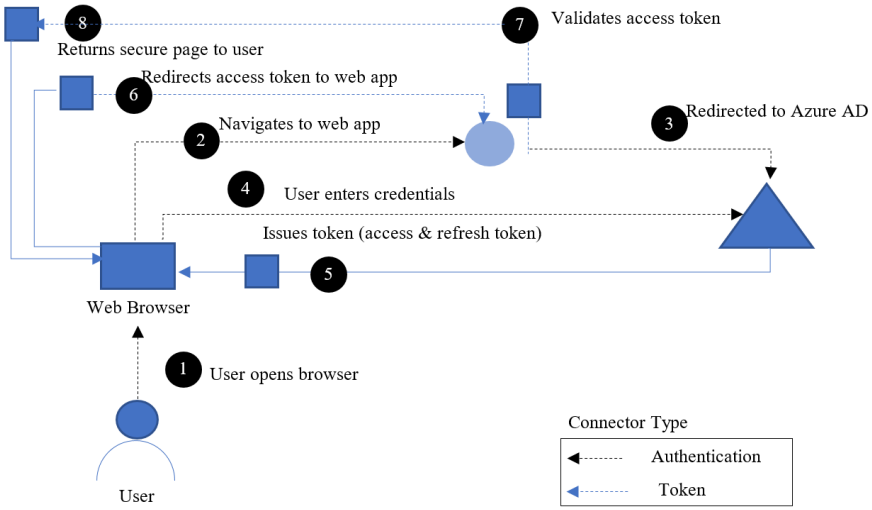

Fig. 4 Authentication for Azure Active Directory Model

Fig 4 contains the main components of the authentication system the user, web browser, web app, and Azure AD. User which contains the service from the web applications. It means the user connected to data allows access through data or resources. The web browser must be interacting with the OAuth Client. Web application, which means the trust authorization server securely authenticates to the client. The authentication server is also called an identity provider, it securely handles the user information and accesses trust relationships. It takes responsibility for issuing the tokens to the grant and revoking to access the resources.

3.4 Open AD Authentication Model

The Active Directory (AD) authentication model is closely related to cryptography because it uses secure methods to confirm the identities of computers and users, protect communication, and protect sensitive data while authentication is taking place. In addition to preventing unwanted access and tampering, the cryptographic protocols utilized in AD are made to guarantee confidentiality, integrity, and authentication. One cryptographic method for safely storing passwords in Active Directory is hashing. Passwords that are created by users are not immediately saved in the Active Directory database. Rather, a one-way cryptographic hash function such as SHA-256 or NTLM hash (for legacy systems) is used to hash it. A fixed-length string that is saved in the AD database is produced by hash functions from an input (such as the password). To prevent passwords from being revealed or sent in plain text, the hashed password is compared to the stored hash when the user logs in. AD can be combined with Multi-Factor Authentication (MFA) systems, which usually use cryptographic techniques like certificate-based authentication and time-based one-time passwords. A cryptographic token created by the program, such as Google Authenticator, is used as second-factor authentication in time-based one-time passwords. Authenticating and using certificates that are stored on the device is known as certificate-based authentication. This type of asymmetric encryption uses public and private keys. Fig:5 represents the authentication procedure for the Open AD Model

Received:August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

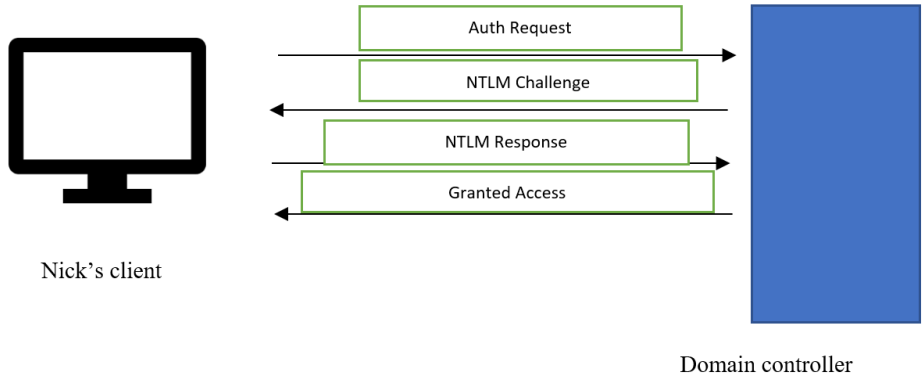

Fig. 5 Authentication for Open AD Model

The authentication working procedure is followed by various steps,

Step 1: Username and passwords are connected to a domain controller.

Step 2: Client creates a password

Step 3: Client sends the request to the domain controller with a username.

Step 4: Domain controller sends the random number as nick client

Step 5: The Client encrypts the challenges used by password and sends the response.

Step 6: Domain controller uses the hash password to encrypt the challenges, which helps to compare to client responses.

Step 7: Completion of authentication provides granted access through response matches.

The limitations of this authentication model as weaker security for specific types of attacks such as NTLM's lack of Single Sign On, and its support for users must repeatedly authenticate to access the different resources. It does not support multifactor authentications. The passwords are stored in hashes, it is the critical elements of authentications. To leak the hashes means mentioning several types of attacks such as pass-the Hash, DCSynuc, and LLMNR poisoning.

3.5 Open LDAP Authentication Model

LDAP is an authentication service followed by the client-server model, this authentication model is followed by the main steps such as user request and non-TLS bind authentications [20]. TCP three-way handshake noted as (SYN, ACK, SYN/ACK). The LDAP blind function should be performed by all types of TCP traffic to the LDAP server, it's typically sent to the port. The protocol communication is covered through a secure socket layer. To introduce the protocol as a simple authentication and security layer used by the various ports.

Received:August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

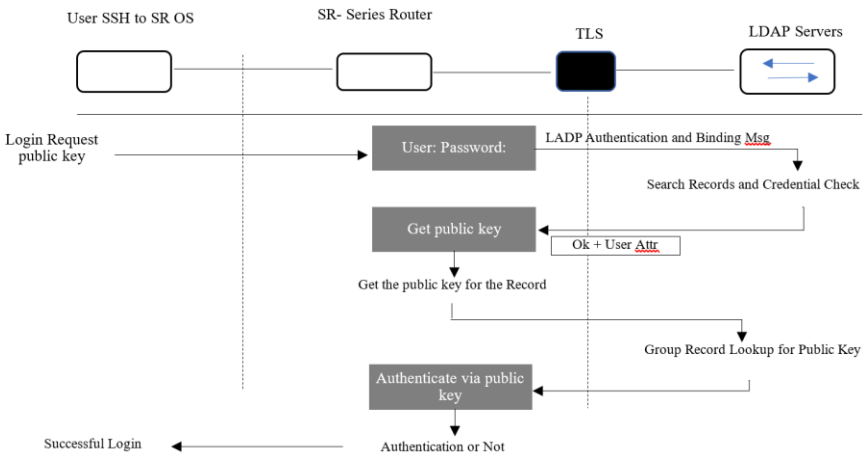

Fig. 6 Open LDAP Authentication Model

Fig. 6 The LDAP authentication model covers user authentication, it helps to verify the user identities before granting access through various resources like a login system. This type of authentication works through the client to the LDAP server, which means credentials are stored. In the implementation stage credentials are matched with one another, and access should be granted. Does not match server should reject the client access. User SSH, which means it's connected to the SR series through secure access. SR series router should act as the network device and login from the user. LDAP server stored the user credentials, and other relevant information required for authentications. This server helps to validate the user identity during the SSH login process. Binding messages SR series authenticate the user sends through public SSH key. This type of key is used to authenticate the user without requiring the password and provide an alternative method of verification. Open LDAP contains the combination of SSH, which allows through SR series to authenticate the user either the passwords. Public key authentication provides flexibility and also enhanced security through network devices. The advantages of the open LDAP authentication model as centralized authentication, scalability, security, open source, and free and extensibility. Disadvantages of this authentication model are a complex setup with maintenance, limited built-in features for modern authentications, performance bottlenecks, and compatibility issues. Followed by this authentication model provides a robust, cost-effective solution and scalable. It is complex to maintain and lacks advanced features with a user interface found by proprietary alternatives. Depending upon this most organizations have technical needs. Open LDAP has an excellent model for authentications [22].

3.6 Database Authentication Model

Database authentication models in cryptography are strategies and tactics used to protect and confirm the identity of systems and users gaining access to a database. It includes protections to guarantee data confidentiality and integrity by limiting access to sensitive information to authorized users or applications. In cryptography, database authentication can be implemented using a variety of models and techniques, usually concentrating on safely storing and sending credentials while guarding against threats such as illegal access or data breaches. The following

Received:August 10, 2025

Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

database authentication models fig: 7 used in cryptography: biometric authentication, two-factor authentication, multi-factor authentication, token authentication, Kerberos authentication, public key infrastructure authentication, and password-based authentication. Identity management system databases come with some features that help with user provisioning, auditing, authorization, authentication, and compliance. Authentication, authorization, user management, integration with identity providers, and password management are examples of these features.

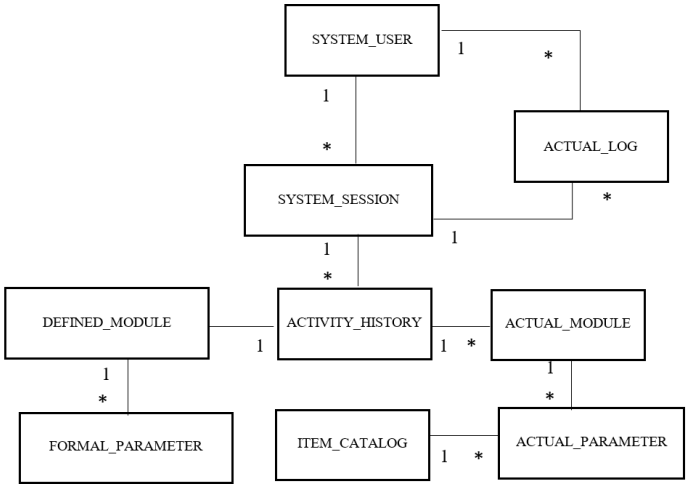

Fig. 7 Database authentication model in PHP

Fig 7 describes the data model, which should be captured and navigated through both successful and unsuccessful logins. A larger module contains the multiple modules against and running time to modules. The actual in the httpd. Applying to one or more protected server parameters is connected to catalog items. To access the log and add to the multiple connections related to single sessions. By establishing a browser's credentials in a realm, basic HTTP/HTTPS authentication works. Browsers can support multiple realms simultaneously. In XHTML documents, realms are defined in the header. They can be manually entered in the form or configured areas, realms serve as protectors for those areas. Basic HTTP/HTTPS authentication has the benefit of requiring no coding for a login or logout feature. The login forms are provided by browsers, and you log out by shutting down every open window. The authentication process operates by checking the credentials against ACL, which means reading the file and comparing the name value related to the user name and password. When the ACL is stored in the database, read the username encrypted to password values from the database table and also compare the results.

Received:August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

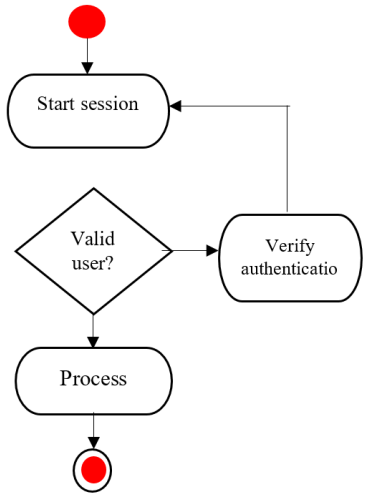

Fig. 8 HTTP/HTTPS Authentication diagram

A realm's authentication is only revoked when all browser windows are closed, according to the basic HTTP/HTTPS authentication model. Figure 8 displays the model's activity diagram as seen within the browser context. Before failing authentication, Microsoft Internet Explorer allows three tries; however, you can get three more consecutive attempts by simply refreshing the page. In contrast, the Firefox browser prompts the user to cancel the authentication process. Entering a URL for the login form initiates a Web application session. The form then posts to the server and sends a message back to the browser asking it to gather and send the user's credentials for validation. The code tries to verify your log credentials when you send them to the SignOnDB.php application. Any webpage in the realm can be used once it's functioning. As previously mentioned, the browser login forms re-prompts when authentication fails.

Authentication Code

```
If ((get_session ($_session[‘sessionid’,$userid,$passwd)==0) ||
(($_session[‘userid’]! = $userid) && ($user id)))
{
// Regerate session ID
Session_regenerare_id(true);
$_SESSION [‘session] = session_id ();
}
Else
{
$authenticated = true;
}
```


Received:August 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Authentication phases

Step 1: User browser sends the message to HTTP request to the server

Step 2: Discover the authentication process and reject the request, respond as authenticate.

Step 3: Save name as login and password combinations.

Step 4: Resend the same request to the same request

Step 5: Request included with to find the login and password

Step 6: To check the password request against to stored database

Step 7: To check HTTP, to permit the document in some groups to reject the request

Step 8: Access the success test in HTML, target program should be run.

Table 3. Security Metric analysis for Kerberos, AD, Azure AD, Open AD, OpenLDAP, and Databases

Authentication Model	Attack Resistance	False Acceptance Rate	Impersonation Rate	Spoofing Detection
Kerberos	Strong Resistance to MITM and replayed attack to ticketing and timestamps. Attack as KDC-compromised Encryption	Low FAR, it's had strong cryptography. Poor key management	Mutual authentication-low impersonation rate. Service ticket requires impersonation.	Reduce spoofing risk and keys are compromised.
Active Directory (AD)	Resistant to MITM due to the Kerberos. Ticker extraction and privilege Escalation	Strong password policies. Increase the NTLM	Low impersonation rate	NTLM related to attacks.
Azure AD	Anti-phishing followed by the account takeover detection. Resistant to traditional attacks.	Low FAR due to MFA security protocols.	Strong authentication practices and to increase the risk.	Adaptive authentications.

Received:August 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Open LDAP	High configurable dependent on proper encryption.	FAR depends upon the password policies. Weak encryption.	Access through admin credentials.	Secured protocols.
Database	SQL injection and misconfigurations.	FAR depends upon the authentication methods.	Admin credentials to access tokens.	Certificate-based authentication. To increase the risk of weak password authentications.

From Table 3 Kerberos and Azure AD generally provide various offers related to low FAR and impersonation rates, it also has the proper key management and user practices. Kerberos has strong ticketing its benefited from cloud features such as MFA with adaptive authentications. AD-related to Kerberos provides a strong relationship between the NTLM relay attacks, but it is not properly configured. The benefits from the AG, which contains the group policies and privilege management. Open LDAP provides flexibility, which is required for strong password policies to avoid vulnerabilities such as LDAP Spoofing. The database has a high level of FAR, and authentication based on SSL certifications provides strong spoofing detections. Spoofing detection is strongly used by encryption more susceptible to spoofing attacks [24].

Table 4. Accuracy metrics used for the Authentication model

Authentication Model	FAR	FRR	TAR	TRR	Accuracy
Kerberos	Low FAR with strong encryption	Low FRR due to mutual authentication for ticket mechanisms.	Strong cryptography with ticketing	High TRR, Kerberos rejects the unauthorized users followed by invalid tickets.	High accuracy with contains the proper implementations.
AD	Low FAR with Kerberos. Pass the Hash attack	Weak passwords or enable the NTLM.	High TAR with Kerberos and MFA-Outdated	Only accept authenticated users.	High accuracy with properly having strong passwords.

Received:August 10, 2025

Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

	mentioned as poor configurations.		authentication models.		
Azure AD	Low FAR, conditional access policies.	Low FRR-Modern authentication protocols.	Adaptive authentications.	Conditional access with adaptive authentications	High accuracy with adaptive authentications.
Open LDAP	Secured configuration (low FAR)	Implemented with proper password and configurations. (Low FAR)	High TAR with SASL	False Rejections.	Moderate to high accuracy.
Database	Low (FAR) used certificate-based authentications.	Low FRR with proper access control.	High TAR used by string user credentials	High TRR followed by IP-based restrictions	High Accuracy with proper access controls.

From Table 4 Accuracy metric analysis, Kerberos and Azer AD provide high accuracy with a low FAR due to the cryptographic protections. These are all offered high TAR due to the strong authentication mechanisms.[25]. AD is achieved through high accuracy it's composed of Kerberos and MFA, here also uses less secure level protocols like NTLM. Open LDAP provides the flexibility required the strong configuration along with high accuracy. It significantly improves both types of FAR and FRR. The database contains certificate-based authentication followed by high accuracy.

4. Evaluation Metrics

Equations 1 to 5 shows the accuracy metrics are used for the authentication model FAR, FRR, TAR, TRR, and Accuracy. FP noted several false positives, with TN as the Number of true negatives. TP is the number of true positives.

False Acceptance Rate (FAR)

$$\mathrm{FAR} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}} \qquad (1)$$

Received:August 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

False Rejection Rate (FRR)

$$\text{FRR} = \frac{\text{FN}}{\text{FN} + \text{TP}} \qquad (2)$$

True Acceptance Rate (TAR)

$$\text{TAR} = \frac{\text{TP}}{\text{TP} + \text{FN}} \qquad (3)$$

True Rejection Rate (TRR)

$$\text{TRR} = \frac{\text{TN}}{\text{TN} + \text{FP}} \qquad (4)$$

Accuracy

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \qquad (5)$$

Table 5. Performance comparison among Authentication models with FAR, FRR, TAR, TRR, and Accuracy

Authentication Model	FAR (%)	FRR (%)	TAR (%)	TRR (%)	Accuracy (%)
Kerberos	0.16	0.16	0.84	0.84	0.84
Active Directory (AD)	0.14	0.14	0.86	0.86	0.86
Azure Active Directory (Azure AD)	0.16	0.16	0.84	0.84	0.84
Open AD	0.16	0.16	0.84	0.84	0.84
Open LDAP	0.26	0.26	0.74	0.74	0.74
Database Authentication	0.18	0.18	0.82	0.82	0.82

To interpret above table 5, a summary of the authentication model followed by some key metrics such as FAR, FRR, TAR, TRR, and Accuracy. FAR, which means the percentage of unauthorized access is incorrectly accepted. FRR, legitimate access incorrectly rejected. TAR, is the percentage of legitimate access correctly accepted, TRR, means unauthorized access to attempt and correctly rejected. Accuracy means to check the overall effectiveness of the authentication system.

Received:August 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

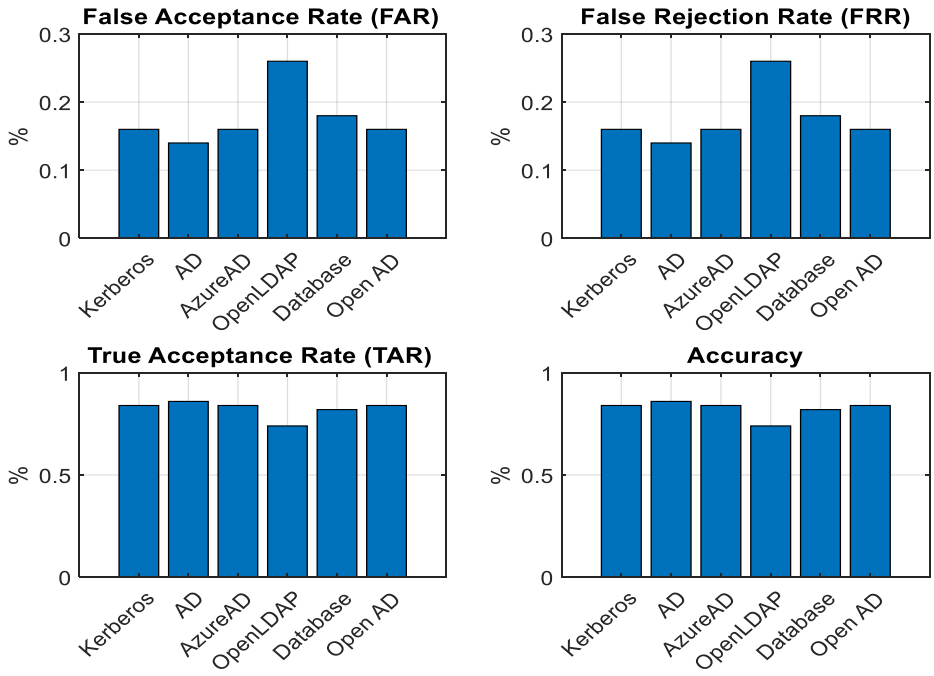

Fig. 9 Performance comparison of Authentication model with FAR, FRR, TAR, TRR, and Accuracy

5. Results and Discussion

The above table (4) and Fig (9) above describe that Kerberos, AD, Azure AD, and Open Ad performed similarly with low FAR and FRR values such as 0.16% compared to others TAR and TRR are very high. The accuracy is as constant as 0.84%. Open LDAP has a high level of FAR and FRR values of 0.26%, resulting in 0.74% compared to TAR and TRR. Based on the overall accuracy result is 0.74%, which is compared to other models. Followed by the database authentication shows the performance is very similar to the Kerberos and AD which contains FAR and FRR as 0.18%, and TAR and TRR as 0.82%. The accuracy result is 0.82%, which is good compared to other types of authentication models. To compare overall analysis, we suggest that Kerberos, AD, Azure AD, and Open AD are equally strong. Open LDAP has lower accuracy it's a concern for high-security applications. Database authentication should be performed by specific database-driven applications. This authentication model has strong accuracy, and security compared to the top-level authentication models. Kerberos and AD are the most reliable authentication tools and provide perfect accuracy with minimal errors. Open LDAP appears to be the less optimal choice along with the terms of security and performance. Database authentication with a good performance, and overall accuracy compared to existing models.

6. Conclusion

An authentication model in an Identity management system is essential for saving the safeguarding data and also ensuring that authorized users can only access the system. This authentication model requires by multi multi-layered approach and balanced through security

Received:August 10, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

with user conveniences. Different types of authentication models are used to provide security in different applications. In the context of cryptography, it is the process of verifying the person's identity that allows access to systems, and applications. To analysis of all authentication models in an Identity management system is essential for analyzing the unique characteristics and providing optimized solutions. Compare all types of authentications with security, scalability, cost, and Ease of integration. Security, which means Kerberos, Azure AD, and AD provide strong security for identity protection. The Open LADP model contains the flexible security required for manual configuration along with advanced features. Scalability, AD, Azure AD with effectively. Ease of integration means these models work as a variety of platforms require customizations. The Open LDAP database model was cost-effective compared to the alternative one. This research compared all authentication models with various metrics. After calculating all metrics, we suggest the result that Kerberos and AD are the most reliable and provide the nearest accuracy with minimal errors. The open LDAP is a less optimal choice in terms of security and performance. Followed by the database authentication has good performance followed by the overall accuracy compared to others

References

[1] Alsirhani, A., Ezz, M., & Mostafa, A. M. (2022). Advanced Authentication Mechanisms for Identity and Access Management in Cloud Computing. Computer Systems Science & Engineering, 43(3). DOI:10.32604/csse.2022.024854

[2] Pillai, N. M., Jayarin, P. J., David, D. B., Jeeva, K., & Kumari, V. S. (2024, March). Algorithm-Driven Optimization of Cloud Computing Architectures for Superior Data Security and Efficiency. In 2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies (pp. 1-4). IEEE. 10.1109/TQCEBT59414.2024.10545176

[3] Uppaluri, V. R. Enterprise Authentication Architectures: Comparing Kerberos, Active Directory, And Okta for Cloud Data Platforms. DOI:10.34218/IJCET_16_01_019

[4] Visumathi, J., & Jesu Jayarin, P. (2015). A secured and reliable biometric user authentication using keystroke template method. *Journal of Applied Security Research*, *10*(3), 375-384. 10.1080/19361610.2015.1038767

[5] Milenković, I., Latinović, O., & Simić, D. (2013). Using Kerberos protocol for single sign-on in identity management systems. JITA-APEIRON, 5(1). DOI:10.7251/JIT1301027M

[6] Alagusabai, A., KAV, R. P., Jayarin, P. J., Jaiganesh, V., & Gopinathan, R. (2022, December). Renewable Energy based Security System for Isolator (Air Brake Switch) using Fingerprint Sensor with Internet of Things. In *2022 International Conference on Automation, Computing and Renewable Systems (ICACRS)* (pp. 1298-1302). IEEE. 10.1109/ICACRS55517.2022.10028991

[7] Bella, G., & Riccobene, E. (1997). Formal Analysis of the Kerberos Authentication System. J. Univers. Comput. Sci., 3(12), 1337-1381. DOI: 10.3217/jucs-003-12-1337

[8] Borse, Y., & Siddavatam, I. (2014). A novel secure remote user authentication protocol using three factors. International Journal of Computer Applications, 975, 8887. DOI:10.5120/15297-3985

Received:August 10, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[9] Pandya, D., Narayan, K. R., Thakkar, S., Madhekar, T., & Thakare, B. (2015). An overview of various authentication methods and protocols. International Journal of Computer Applications, 131(9), 25-27. DOI:10.5120/ijca2015907389

[10] Baqer, K., Bezuidenhoudt, J., Anderson, R., & Kuhn, M. (2017). SMAPs: short message authentication protocols. In Security Protocols XXIV: 24th International Workshop, Brno, Czech Republic, April 7-8, 2016, Revised Selected Papers 24 (pp. 119-132). Springer International Publishing. https://doi.org/10.17863/CAM.7636

[11] Mitchell, J. C., Roy, A., Rowe, P., & Scedrov, A. (2008). Analysis of EAP-GPSK authentication protocol. In Applied Cryptography and Network Security: 6th International Conference, ACNS 2008, New York, NY, USA, June 3-6, 2008. Proceedings 6 (pp. 309-327). Springer Berlin Heidelberg. DOI:10.1007/978-3-540-68914-0_19

[12] Du, L. P., Li, Y., Xu, G. N., & Duan, F. (2013). Research on micro-certificate-based security systems for the Internet of Things. Applied Mechanics and Materials, 263, 3125-3129. DOI:10.4028/www.scientific.net/AMM.263-266.3125

[13] R, Rajesh & Kannan, Aaditya & Nair, Adithya & Narayan, Adittya & M, Sarvesh & Vetrivendan, Varun. (2024). Secure Web Authentication Using Visual Cryptography. 1-6. DOI:10.1109/ICSCAN62807.2024.10894432

[14] Prakash, A., & Kumar, U. (2018). Authentication protocols and techniques: a survey. Int. J. Comput. Sci. Eng, 6(6), 1014-1020. DOI:10.26438/ijcse/v6i6.10141020

[15] Uppaluri, Vivekananda & Pub, Research. (2025). Enterprise Authentication Architectures: comparing kerberos, active directory, and okta for cloud data platforms. International Journal of Computer Engineering & Technology. 16. 210-219. DOI:10.34218/IJCET_16_01_019

[16] Luu, Huan & Nguyen, Duy-Minh & Pham, Hoang-Anh & Huynh Tuong, Nguyen. (2020). Authentication in E-learning systems: Challenges and Solutions. Science & Technology Development Journal - Engineering and Technology. 3. SI95-SI101. DOI:10.32508/stdjet.v3iSI1.516

[17] Kadlec, J., Jaros, D., & Kuchta, R. (2010, September). Implementation of an Advanced Authentication Method within Microsoft Active Directory Network Services. In 2010 6th International Conference on Wireless and Mobile Communications (pp. 453-456). IEEE. DOI: 10.1109/ICWMC.2010.48

[18] Subbarao, D., Raju, B., Anjum, F., Rao, C. V., & Reddy, B. M. (2023). Microsoft Azure active directory for next-level authentication to provide a seamless single sign-on experience. Applied Nanoscience, 13(2), 1655-1664. DOI:10.1007/s13204-021-02021-0

[19] Haimed, Ibrahim & Albahar, Marwan & Alzubaidi, Ali. (2023). Exploiting Misconfiguration Vulnerabilities in Microsoft's Azure Active Directory for Privilege Escalation Attacks. Future Internet. 15. 226. DOI:10.3390/fi15070226

[20] Chandra, J. V., Challa, N., & Pasupuletti, S. K. (2019). Authentication and authorization mechanism for cloud security. International Journal of Engineering and Advanced Technology, 8(6), 2072-2078. DOI:10.35940/ijeat.F8473.088619

[21] Yousefnezhad, Narges & Filippov, Roman & Javed, Asad & Buda, Andrea & Madhikermi, Manik & Främling, Kary. (2017). Authentication and Access Control for Open Messaging Interface Standard. 20-27. DOI:10.1145/3144457.3144461

[22] Ibrahim, A., & Ouda, A. (2016, October). Innovative data authentication model. In 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 1-7). IEEE. DOI: 10.1109/IEMCON.2016.7746268

Received:August 10, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[23] Ferrag, M. A., Maglaras, L., Derhab, A., & Janicke, H. (2020). Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues. Telecommunication Systems, 73(2), 317-348. DOI:10.48550/arXiv.1803.10281

[24] Subbarao, D. & Raju, Bhagya & Anjum, Farha & Rao, Ch & Reddy, B. (2021). Microsoft Azure active directory for next level authentication to provide a seamless single sign-on experience. Applied Nanoscience. 13. DOI:10.1007/s13204-021-02021-0

[25] Shridhar, R., & Udayakumar, R. (2024). Developing A Tourism Information Portal Using Web Technologies and Database Management. Indian Journal of Information Sources and Services, 14(3), 71–76. https://doi.org/10.51983/ijiss-2024.14.3.10.

Received:August 10, 2025