

A Comprehensive Review of User Authentication and Authorization Techniques in Cloud Computing

Dr Chintal Kumar Patel¹

¹ Associate Professor, CSE, Geetanjali Institute of Technical Studies, India

ABSTRACT: Cloud computing has emerged as a transformative paradigm for delivering scalable, flexible, and cost-effective computing services over the Internet. As organizations increasingly rely on cloud platforms for data storage, application hosting, and resource management, ensuring secure access to cloud resources has become a critical challenge. Authentication and authorization mechanisms play a fundamental role in protecting cloud environments by verifying user identities and regulating access privileges. This paper presents a comprehensive review of user authentication and authorization techniques in cloud computing. The study examines widely adopted authentication approaches, including password-based, multi-factor, biometric, and behavioral authentication methods, as well as authorization models such as Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Mandatory Access Control (MAC). Furthermore, recent advancements in artificial intelligence-driven authentication, fine-grained access control, graphical authentication systems, and cloud security frameworks are reviewed and analyzed. The findings indicate a significant transition from traditional security mechanisms toward intelligent, adaptive, and context-aware solutions that enhance security, usability, and access management. The review highlights that multi-factor authentication, biometric technologies, behavioral analytics, and attribute-based authorization frameworks offer improved protection against evolving cyber threats and represent promising directions for securing modern cloud computing environments.

KEYWORDS: Cloud Computing, User Authentication, User Authorization, Multi-Factor Authentication (MFA), Biometric Authentication, Access Control, Cloud Security.

1. Introduction

The development of cloud computing has significantly changed how the IT sector functions today. Cloud computing makes it possible to investigate better IT services with lower expenses and less investment. The popularity of software as a service has increased because of cloud computing's impact on how IT hardware is developed and procured. It is an internet-based technology that gives users access to server-stored data as a service whenever they want [1][2]. Cloud computing offers IIoT environments the scalability, flexibility, and computational power needed to process and store the data collected from diverse devices and sensors. Its ability to centralize operations and provide on-demand resources enables industries to optimize workflows and enhance decision-making processes. By reducing the need for extensive on-premises infrastructure, cloud computing also lowers costs and allows organizations to focus on their core operations while benefiting from advanced technological capabilities [3].

Cloud authentication verifies user identities across a cloud platform to determine whether the user is trusted to access cloud applications, data, services, and resources by ensuring access rights and privileges [4][5]. The lack of strong and appropriate cloud authentication techniques leads to the occurrence of some cloud security threats and attacks [6]. Some of the most common cloud threats are information disclosure, Denial-of-Service (DoS) attacks, identity spoofing, data tampering, repudiation, account hijacking, and the elevation of privileges [7][8]. Cloud-based authentication attacks include DoS attacks, Man-in-the-Middle (MITM) attacks, Replay attacks, Cloud Malware Injection attacks, and Password Discovery attacks.

Cloud-native architecture refers to a set of practices and technologies that enable the development and deployment of applications in the cloud [9]. It is an approach that emphasizes using microservices, containers, and container orchestration platforms such as Kubernetes. Cloud-native architecture is designed to take

advantage of the cloud's scalability, flexibility, and agility[10]. It allows applications to be built and deployed faster and with greater reliability than traditional approaches, and it also enables organizations to better manage their resources and reduce costs.

Among all cloud computing security techniques, access control (AC) plays an important role in preserving the integrity of information by limiting alterations to resources only to legitimate users. In addition, access control protects confidentiality by ensuring that data are disclosed only to customers who are authorized to access them [11]. Furthermore, access control protects resources from unauthorized users launching denial-of-service attacks. Authentication is a primary security service; the most commonly used procedure is the verification of a username and password. It is the process of verifying who a user is, whereas authorization is the process of determining the level of access granted to authenticated users. Auditing consists of examining previous activities to determine whether security violations have occurred [12]. Audit data are recorded in audit log files, and continuous monitoring and auditing procedures should be followed by an intelligent system for securing the cloud.

To strengthen cloud security, various authentication and authorization techniques have been proposed, including password-based authentication, multi-factor

authentication (MFA), biometric authentication, token-based authentication, and role-based or attribute-based access control mechanisms. These techniques aim to ensure secure identity verification, regulate resource access, and protect cloud environments from evolving cyber threats. Therefore, a comprehensive review of user authentication and authorization techniques is essential to understand recent advancements, challenges, and future research directions in cloud computing security.

A. Structure of the Paper

This paper is structured as follows: Section II covers cloud fundamentals, including service and deployment models. Section III reviews authentication methods like password-based, multi-factor, biometric, and behavioral techniques. Section IV discusses authorization frameworks such as RBAC, ABAC, and MAC. Section V presents recent literature and advancements. Section VI concludes with key insights and future research directions.

2. Cloud Computing and Its Service Models

Cloud computing is a technology that delivers a new model form existing grid technology and is based on internet resources sharing and broad network access [13]. Cloud computing model is composed of five essential cloud characteristics, namely on demand self-services, Broad network access, Independent resources pooling, Rapid elasticity, and Measured service [14].

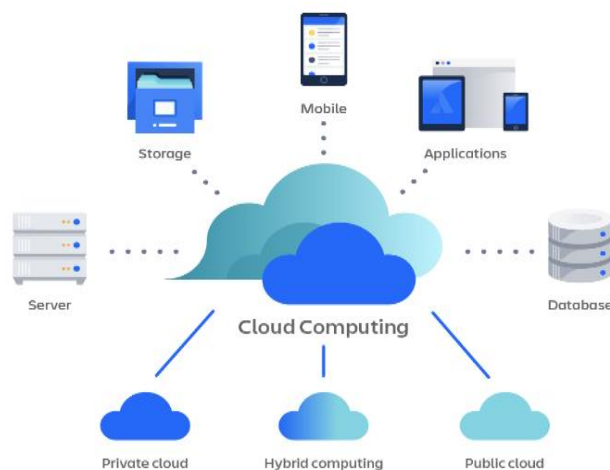


Fig. 1. Cloud Computing Work

Figure 1 illustrates the fundamental architecture of cloud computing, where centralized cloud resources provide storage, applications, servers, and databases through private, public, and hybrid cloud models [15]. This interconnected framework enables scalable, flexible, and efficient access to computing services and resources over the internet.

There are some cloud computing service models as follows:

- **Software as a Service (SaaS):** SaaS is one of the
- **Infrastructure as a Service (IaaS):** Infrastructure as

cloud subscription service groups, along with IaaS and PaaS. It allows businesses to access the programs they need without having to host them on their own servers [16]. It has grown in popularity since it eliminates the need for organizations to buy servers and other resources, as well as retain an in-house support team. Instead, a SaaS provider hosts their applications and provides SaaS security and maintenance. Most business product providers, such as the Oracle Financials Cloud, also sell cloud implementations of their applications.

a service (IaaS) is a single-tenant model where the cloud computing service provider dedicates resources that are only shared with contracted consumers based on pay-per-use fees [17]. The IaaS model helps to minimize the need for a large initial investment in computing hardware such as networking devices, processing power, and servers.

- **Platform as a Service (PaaS):** enables users to develop in the Cloud environment the users' applications created using libraries, services, and APIs compatible with the Cloud provider. Users cannot directly manage or control the infrastructure beneath the Cloud, including networks, servers, operating systems, or storage, but retain control of the deployed applications and specific configuration settings for the application-hosting domain.

3. User Authentication Techniques in Cloud

Computing

User authentication techniques in cloud computing ensure that only legitimate users gain access to cloud-based resources [18]. These techniques vary in complexity, security level, and usability, often depending on the sensitivity of the data and services involved.

A. Password-Based Authentication

The use of passwords is an important authentication method to protect user information in the field of information security. When users choose passwords, security and convenience mutually conflict. For example, while a password that is composed in a complicated manner by combining uppercase and lowercase letters, numbers, and special symbols, such as "Qw3@lv53", is safe since it cannot be easily inferred by other users, it is inconvenient to use because it cannot be easily remembered by the user [19].

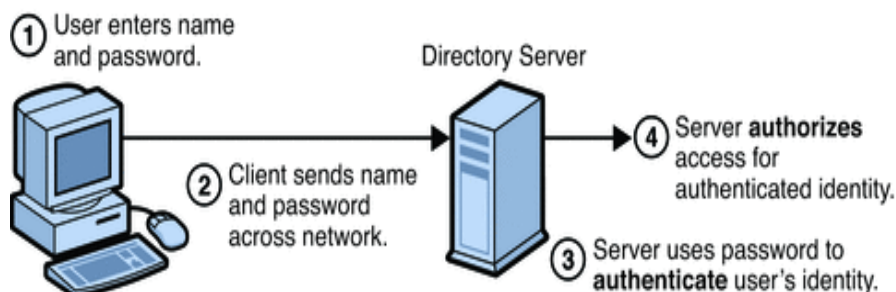


Fig. 2. Password-Based Authentication in Cloud

Password-based authentication remains one of the most widely used mechanisms for verifying user identity in cloud environments. As shown in Figure 2, user credentials are transmitted to a directory server for validation, after which authorized users are granted secure access to cloud resources.

- **Text-Based Password:** Despite many weaknesses, user authentication through textual passwords has been widely used for a long time. In a textual password scheme, credentials are directly inserted into login fields, which results in easy capture of password through spyware attack, and shoulder Surfing attack [20]. Another problem with textual

password schemes is that users tend to set short, easy-to-remember passwords, which are easy to crack through brute-force or dictionary attacks. Therefore, users are restricted from adding numbers or special characters in their passwords, but such policies make the passwords hard to remember.

- **Graphical Password Authentication:** Graphical passwords refer to using pictures (also drawings) as passwords. In theory, graphical passwords are easier to remember, since humans remember pictures better than words. Also, they should be more resistant to brute-force attacks, since the search space is practically infinite an example shown in Figure 3 [21].

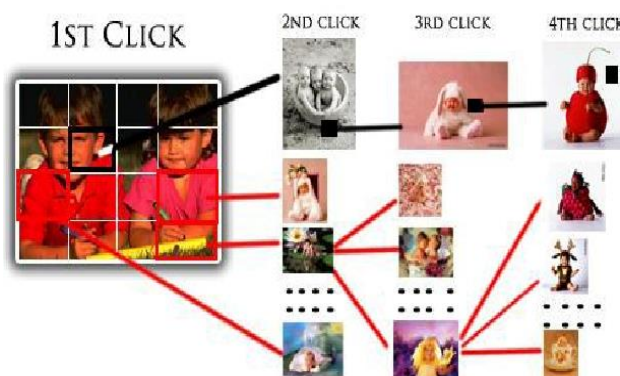


Fig. 3. Graphical Password Authentication

B. Multi-Factor Authentication (MFA)

Security vulnerabilities of traditional single factor authentication have become a major concern for security practitioners and researchers. To mitigate single point failures, new and technologically advanced Multi-Factor Authentication (MFA) tools have been developed as security solutions. However, the usability and adoption of such tools have raised concerns. An obvious solution can be viewed as conducting user

studies to create more user-friendly MFA tools [22]. A common example of MFA usage in an everyday activity is using an ATM with a bank card (something the user has) and PIN (something the user knows) [23].

An integration of novel solutions has always been a major challenge for both developers and managers [24]. The key challenges are usability, integration and privacy/Security in the first place, user acceptance is a critical aspect for the adoption of strong identity and multi-factor authentication.



Fig. 4. Multi Factor Authentication

The concept of MFA is illustrated in Figure 4. The diagram shows that combining a standard user password with secondary verification factors—such as biometric fingerprints or mobile security codes—is required to successfully grant system access.

1) Usability

The main usability challenges emerging in the authentication process could be characterized from three perspectives:

- **Task efficiency:** time to register and time to authenticate with the system;
- **Task effectiveness:** the number login attempts to authenticate with the system;
- **User preference:** whether the user prefers a particular authentication scheme over another [24].

2) Integration

There are six steps of the Integration as follows:

- **User Authentication:** User requests access to resources-Identity Access Management (IAM) verifies user identity through enabled MFA.
- **Device Verification (access only for trusted devices):** To determine: Look up device trust assessment to determine compliant, current and secure.
- **Application Access:** User request access to an application- IAM determine if app trust is verified Micro-segmentation (dividing network into small segments) to increase security by limiting threats to a compromised segment only without affecting other

segments.

- **Continuous monitoring:** Detect suspicious activity, monitor traffic and user behavior, modify access control vigorously as needed.
- **Least Privilege access:** Access permitted for specific roles and responsibilities where users and devices are granted only the minimum access to complete their tasks (reduces potential impact if breached).
- **Adaptive Access Policies with MFA:** Through contextual factors like location, behavior, security posture, allow for adjusting the authentication mechanism dynamically [25].

3) Privacy/Security

The proposed framework introduces new security risks, such as vulnerabilities in the authentication method selector (AMS) technique or the intrusion detection component[6]. Additionally, the framework collects sensitive user data, such as location and web browser information, which could be misused if compromised the proposed framework collects sensitive user data, such as location and web browser information. These data could be misused if compromised. Additionally, the framework uses these data to manipulate user behavior, which could be seen as an invasion of privacy.

C. Biometric Authentication

A biometric system uses measurements of an individual's personal biological makeup or distinctive behaviors to identify them by comparison to biometric collection models of the same kind [26]. It is categorized as a recognition or validation system at the moment, and

it can be described as a computerized method of determining or validating an individual's appearance based on specific physiological or behavioral characteristics.

• **Types of Biometric Authentication Technologies:** There are some major techniques of biometric authentications as given below:

• **Fingerprint Recognition:** Fingerprint based biometric authentication systems became one of the most conducted, popular and successful authentication techniques among other biometrics security methods for both of identification and verification processes of one's identity [27].

• **Face Recognition:** The facial features (eyes, nose, lips and chin) of human have played a significant role in the recognition of individuals for long time. Depending on the unique shaping of each person's face, it has been a popular method in biometric recognition area.

• **Iris Recognition:** Iris is that colored circular part that is located in center of the eye. The distinctiveness of iris pattern provides an effective recognition scheme of individuals. Based on the biological composition of the iris, it has a specific network of tissues that are visibly recognized. However, an individual's iris forms over the first year of the life when the iris characteristics cannot be genetically changed.

• **Retina Recognition:** In each person's eye, the retina is that layer that is made of a complicated network of neural cells at the back of the eye. This part has a unique feature for each retina due to the

complicated capillaries that are responsible for providing the retina with blood.

• **Hand Geometry Recognition:** Many security systems and applications depend on the recognition of hand geometry as an automated technique for the identification/verification of their legitimate users. This biometric authentication method started gaining wide popularity in various security sectors.

• **Ear Recognition:** Another biometric authentication technique is conducted based on the recognition of the unique shape and appearance of human being ear [27]. Naturally, a person is born with a visual shape of his/her ears.

D. Behavioral Authentication

The advantages of friction lessness, continuousness, synthesizability, and inherence in behavioral authentication have attracted significant attention from the security research community. Narrowly defined, behavioral authentication usually refers to behavioral identity authentication [28]. It is a technology that has emerged as a result of the continuous development of the artificial intelligence industry and the improvement of computing and storage capabilities in hardware.

Behavioral biometrics rely on user interaction patterns, such as swipe dynamics, typing speed, and touch pressure, to enable continuous authentication [29]. Unlike static physiological biometrics, behavioral methods are dynamic and adaptive to changes in user behavior over time, and this, in turn, provides resilience against spoofing attempts and adversarial attacks, as summarized in Table I.

TABLE I. COMPARATIVE OVERVIEW OF USER AUTHENTICATION TECHNIQUES

Criteria	Password-Based	Multi-Factor Authentication (MFA)	Biometric Authentication	Behavioral Authentication
Authentication Factors	Something you know	Combination (e.g., password + OTP/biometric)	Something you are (fingerprint, face, iris)	Something you do (keystroke, gait, mouse movement)
Security Level	Low (easily guessed or stolen)	Moderate to High (depends on factor strength)	High (unique to user, hard to fake)	Moderate (can be spoofed or vary with context)
Usability	High (simple to use, familiar)	Moderate (extra step may annoy users)	High (quick and easy, especially on mobile)	Moderate (runs in background, may vary in accuracy)
Implementation Cost	Low	Moderate (need for tokens, SMS gateways, etc.)	High (hardware sensors, software integration)	Moderate (machine learning models, data capture)
Accuracy	Low (prone to human error)	Depends on factors used	High (modern sensors have <1% error rate)	Varies (depends on environment & behavior changes)
Common Attacks	Phishing, brute force, reuse	MITM, token theft, SIM swap	Spoofing (face masks, fake fingerprints)	Mimicry, adversarial ML
User Experience	Simple but insecure	Secure but slightly more complex	Seamless on modern devices	Passive, no user effort

Use Cases	Basic logins, legacy systems	Online banking, cloud services	Mobile unlocking, secure workstations	Continuous authentication, fraud detection
-----------	------------------------------	--------------------------------	---------------------------------------	--

4. User Authorization Techniques

User authorization is the process of determining whether a user has the necessary permissions to access

or perform actions on a specific resource after they have been authenticated. While authentication answers “Who are you?”, authorization answers “What are you allowed to do” as mentioned in Figure 5.



Fig. 5. User Authorization view

A. Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) is a promising method for managing sets of access rights, offering simplified maintenance, unlike DAC and MAC, which are rarely enforced in open networks [30]. RBAC, which emerged in the 1970s in multi-user and multi-application online systems, grants permissions to roles rather than individuals, and users obtain permissions by assuming roles.

B. Attribute-Based Access Control (ABAC)

Attribute-Based Access Control (ABAC) is an emerging form of access control that is starting to garner interest in both recent academic literature and industry application [31]. While there is currently no single agreed upon model or standardization of ABAC, there are commonly accepted high level definitions and descriptions of its function.

C. Mandatory Access Control (MAC)

An efficient MAC protocol should be able to avoid simultaneous transmissions from multiple IoT nodes. Otherwise, a packet collision occurs at the receiver side, resulting in the destruction of all collided packets. Several MAC solutions for IoT applications have been proposed to achieve a perpetual operation among the nodes [32].

5. Literature Review

This section reviews recent advancements in user authentication and authorization techniques in cloud

computing, emphasizing AI-driven authentication, fine-grained access control, cloud security frameworks, multi-tenant authorization, graphical authentication methods, and secure resource management approaches aimed at enhancing cloud security, scalability, and user privacy.

T. Ali, M. Al-Khalidi, and R. Al-Zaidi (2026) Examines the various classification and categorization schemes for cloud computing security issues, including the widely known CIA trinity (confidentiality, integrity, and availability), by considering critical aspects of the cloud, such as service models, deployment models, and involved parties. A comprehensive comparison of cloud security classifications constructs an exhaustive taxonomy. ISO27005, NIST SP 800–30, CRAMM, CORAS, OCTAVE Allegro, and COBIT 5 are rigorously compared based on their applicability, adaptability, and suitability within a cloud-based hosting methodology [33].

P. Pandey (2025) presents an AI-enabled Multi-Factor Authentication (MFA) framework that enhances cloud security by leveraging AI techniques for behavioral analysis, anomaly detection, and dynamic decision-making. Using real-world datasets, this framework extracts user behavior, device characteristics, and contextual information to evaluate authentication requests dynamically [34].

M. Z. Khan et al., (2024) study outlines a comprehensive cloud authorization framework explicitly designed to address the unique challenges posed by the dynamic nature of big data processing in cloud environments. The proposed prototype / framework integrates advanced authentication and authorization

mechanisms tailored to the characteristics of big data systems, including distributed processing, heterogeneous data sources, and diverse user access patterns. Leveraging scalable cloud infrastructure and advanced cryptographic techniques, the framework ensures granular access control and data protection throughout the data lifecycle [35].

Z. Cheng et al. (2024) explores data authorization and access technologies in multi-tenant environments, employing SQL dynamic substitution strategies to ensure fine-grained data authorization control in a multi-tenant environment. This allows a single system codebase to switch freely between tenants with the same database structure without modifying the SQL [36].

R. Khedkar et al. (2024) discusses about the various dimensions of a graphical authentication system, including privacy, threat detection and access control mitigation, encryption, and user awareness. Authentication system graphics proved to be an

innovative alternative to traditional alphanumeric passwords to improve user security and convenience. Dive into knowledge-based authentication, which includes picture passwords that are said to be more convenient for humans to remember passwords [37].

N. Li et al. (2023) primarily investigates the collaboration of AI inference computation between mobile devices and base stations, with a specific focus on the joint optimization of communication and computing resources in a multi-user environment. A communication and computing integrated scheduling algorithm are proposed to ensure optimal system performance in terms of inference accuracy and computation latency [38].

Table II summarizes recent studies on cloud authentication and authorization techniques, highlighting methodologies, key findings, limitations, challenges, and future directions for secure cloud access management.

TABLE II. SUMMARY OF THEE STUDY ON USER AUTHENTICATION AND AUTHORIZATION TECHNIQUES IN CLOUD COMPUTING

Reference	Study On	Approach	Key Findings	Challenges / Limitations	Future Directions
T. Ali et al. (2026)	Cloud security classification and risk assessment	Comparative analysis of cloud security taxonomies and risk management frameworks	Developed a comprehensive taxonomy of cloud security issues and compared major risk assessment models	Limited focus on real-time adaptive authentication and authorization mechanisms	Integration of dynamic security assessment with intelligent access control frameworks
P. Pandey (2025)	AI-enabled Multi-Factor Authentication (MFA)	AI-based behavioral analysis, anomaly detection, and adaptive authentication	Improved authentication accuracy through contextual and behavioral intelligence	Privacy concerns, computational overhead, and scalability challenges	Lightweight and privacy-preserving AI-driven authentication models
M. Z. Khan et al. (2024)	Authorization framework for cloud-based big data	Advanced authentication, authorization, and cryptographic techniques	Enabled granular access control and secure data lifecycle management	Complexity of managing heterogeneous users and large-scale data environments	Scalable and decentralized authorization frameworks for distributed clouds
Z. Cheng et al. (2024)	Data authorization in multi-tenant cloud environments	SQL dynamic substitution-based fine-grained access control	Improved tenant isolation and flexible authorization management	Potential performance degradation and limited adaptability to dynamic access requirements	Intelligent and context-aware access control mechanisms for multi-tenant systems
R. Khedkar et al. (2024)	Graphical authentication systems	Knowledge-based graphical password techniques	Enhanced usability and memorability compared to text passwords	Vulnerability to shoulder surfing and user behavior-based attacks	Hybrid graphical-biometric authentication solutions with stronger security guarantees
N. Li et al. (2023)	AI-assisted resource scheduling for	Joint communication and computing	Reduced latency and improved inference	Focuses on resource allocation rather	Integration of resource management with

	cloud-edge systems	resource optimization	accuracy in multi-user environments	than authentication and authorization security	secure identity and access control frameworks
--	--------------------	-----------------------	-------------------------------------	--	---

6. Conclusion and Future Work

Cloud computing has become a fundamental technology for delivering scalable, flexible, and cost-effective services across diverse application domains. However, the increasing reliance on cloud environments has elevated the importance of robust authentication and authorization mechanisms for protecting sensitive resources and user data. This review examined major user authentication techniques, including password-based, multi-factor, biometric, and behavioral authentication, along with authorization models such as RBAC, ABAC, and MAC. The analysis revealed that traditional password-based approaches alone are insufficient against evolving cyber threats, whereas multi-factor and biometric authentication provide stronger security and improved identity assurance. Furthermore, advanced authorization frameworks, particularly attribute-based models, offer more flexible and fine-grained access control for dynamic cloud environments. The reviewed literature also highlights the growing integration of artificial intelligence and behavioral analytics to enhance authentication accuracy, adaptive access control, and overall cloud security. These advancements demonstrate a clear shift toward intelligent, context-aware, and user-centric security solutions for modern cloud infrastructures.

Future research should focus on developing lightweight and privacy-preserving authentication frameworks that integrate artificial intelligence, behavioral analytics, and adaptive access control mechanisms. Additionally, improving scalability, interoperability, and resistance to emerging cyberattacks will be essential for securing next-generation cloud computing environments.

REFERENCES

1. B. Uzoma and B. Okhuoya, "A Research On Cloud Computing," 2022.
2. J. B. Mehta, "AI-Driven Test Engineering for Cloud-Native Systems," *Int. J. Data Sci. IoT Manag. Syst.*, vol. 5, no. 1, Jan. 2026, doi: 10.64751/ijdim.2026.v5i1.297.
3. E. Dritsas and M. Trigka, "A Survey on the Applications of Cloud Computing in the Industrial Internet of Things," *Big Data Cogn. Comput.*, vol. 9, no. 2, 2025, doi: 10.3390/bdcc9020044.
4. J. B. Mehta, "Autonomous Patch Validation For Zero-Day Exploits In Enterprise Clouds," *Int. J. Appl. Math.*, vol. 38, no. 4s, pp. 1270–1285, Oct. 2025, doi: 10.12732/ijam.v38i4s.685.
5. M. Parikh, A. A. Soni, S. M. Shah, and A. R. Jha, "Big Data Workload Profiling for Energy-Aware Cloud Resource Management," in 2026 International Conference on Data Analytics for Sustainability and Engineering Technology (DASET 2026)), Track: Big Data and Machine Learning Applications, IEEE, Ed., arXiv preprint arXiv, 2026, pp. 01–07, januray. doi: 10.48550/arXiv.2601.11935.
6. A. M. Mostafa et al., "Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication," *Appl. Sci.*, vol. 13, no. 19, 2023, doi: 10.3390/app131910871.
7. R. Lingam, S. Nagi, M. Chigurupati, and B. T. Myneni, "Resilient DevSecOps: Self-Healing Cloud-Native Systems via SRE-Driven AI Threat Detection and Response," in 2026 International Conference on Smart Futuristic Technology, IEEE, Jan. 2026, pp. 1–6. doi: 10.1109/ICSFT66733.2026.11508049.
8. M. Kumar and M. K. Shah, "AI-Driven DDoS Detection for Network Security: A Performance Analysis of Machine-Deep Learning Methods on Network Traffic Data," in 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC), Houston, TX, USA: IEEE, Feb. 2026, pp. 1–6. doi: 10.1109/ICAIC67076.2026.11395710.
9. R. K. Gadiraju, "Cloud-Native AI Platforms for Scalable Enterprise Machine Learning: Architecture, Challenges, and Best Practices," *Int. J. ofINTELLIGENT Syst. Appl. INENGINEERING*, vol. 9, no. 4, pp. 481–492, October, 2021.
10. M. S. Rahaman, S. N. Tisha, E. Song, and T. Cerny, "Access Control Design Practice and Solutions in Cloud-Native Architecture: A Systematic Mapping Study," *Sensors*, vol. 23, no. 7, 2023, doi: 10.3390/s23073413.
11. A. Mohammad, "Distributed Authentication and Authorization Models in Cloud Computing Systems: A Literature Review," *J. Cybersecurity Priv.*, vol. 2, no. 1, pp. 107–123, 2022, doi: 10.3390/jcp2010008.
12. D. Chandra Jadala, "Authentication and Authorization Mechanism for Cloud Security," *Int. J. Eng. Adv. Technol.*, vol. 8, no. 6, pp. 2072–2078,

- Aug. 2019, doi: 10.35940/ijeat.F8473.088619.
13. A. Joon, B. K. R. Janumpally, A. Gogineni, and P. Chatterjee, "Efficient Large-Scale Intrusion Identification and Prevention in Distributed Cloud Networks Using Artificial Intelligence," in 2025 5th International Conference on Intelligent Technologies (CONIT), HUBBALLI, India: IEEE, 2025, pp. 1–8, September. doi: 10.1109/CONIT65521.2025.11167760.
 14. V. Mohan and s Sathyanathan, "Research in Cloud Computing-An Overview," *Int. J. Distrib. Cloud Comput.*, vol. 3, 2015, doi: 10.21863/ijdcc/2015.3.1.002.
 15. H. N. Dholariya, "Regulatory-Grade Autonomous Data Modernization: The RAMA Framework for Compliance-Aware AI-Native Cloud Architectures," *J. Comput. Anal. Appl.*, vol. 35, no. 1, pp. 883–898, Jan, Jan. 2026, doi: 10.48047/jocaaa.2026.35.01.40.
 16. M. Humayun, M. Niazi, M. F. Almufareh, N. Z. Jhanjhi, S. Mahmood, and M. Alshayeb, "Software-as-a-Service Security Challenges and Best Practices: A Multivocal Literature Review," *Appl. Sci.*, vol. 12, no. 8, p. 3953, Apr. 2022, doi: 10.3390/app12083953.
 17. Y. Alghofaili, A. Albattah, N. Alrajeh, M. A. Rassam, and B. A. S. Al-rimy, "Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges," *Appl. Sci.*, vol. 11, no. 19, 2021, doi: 10.3390/app11199005.
 18. R. K. Gadiraju, "Artificial Intelligence for Resource Optimization in Cloud Computing Environments," *J. Electr. Syst.*, vol. 20, no. 6, pp. 3164–3174, March, 2024.
 19. K. H. Hong and B. M. Lee, "A Deep Learning-Based Password Security Evaluation Model," *Appl. Sci.*, vol. 12, no. 5, 2022, doi: 10.3390/app12052404.
 20. S. Zaman, S. Raheel, T. Jamil, and M. Zalisham, "A Text based Authentication Scheme for Improving Security of Textual Passwords," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, 2017, doi: 10.14569/IJACSA.2017.080771.
 21. A. Almulhem, "A graphical password authentication system," in 2011 World Congress on Internet Security (WorldCIS-2011), IEEE, Feb. 2011, pp. 223–225. doi: 10.1109/WorldCIS17046.2011.5749855.
 22. S. Das, B. Wang, Z. Tingle, and L. J. Camp, "Evaluating User Perception of Multi-Factor Authentication: {A} Systematic Review," *CoRR*, vol. abs/1908.0, 2019.
 23. J. Williamson and K. Curran, "Best Practice in Multi-factor Authentication," *Semicond. Sci. Inf. Devices*, vol. 3, 2021, doi: 10.30564/ssid.v3i1.3152.
 24. A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-Factor Authentication: A Survey," *Cryptography*, vol. 2, no. 1, 2018, doi: 10.3390/cryptography2010001.
 25. H. Ramcharan, "The Effective Integration of Multi-Factor Authentication (MFA) with Zero Trust Security," *Am. J. Math. Comput. Model.*, vol. 10, pp. 1–5, 2025, doi: 10.11648/j.ajmcm.20251001.11.
 26. K. Modi and L. Devaraj, "Advancements in Biometric Technology with Artificial Intelligence," 2023.
 27. I. Alsaadi, "Physiological Biometric Authentication Systems, Advantages, Disadvantages And Future Development: A Review," *Int. J. Sci. Technol. Res.*, vol. Volume 4, 2015.
 28. C. Wang, H. Tang, H. Zhu, J. Zheng, and C. Jiang, "Behavioral authentication for security and safety," *Secur. Saf.*, vol. 3, 2024, doi: 10.1051/sands/2024003.
 29. M. L. Shuwandy et al., "A Robust Behavioral Biometrics Framework for Smartphone Authentication via Hybrid Machine Learning and TOPSIS," *J. Cybersecurity Priv.*, vol. 5, no. 2, 2025, doi: 10.3390/jcp5020020.
 30. J. Singh, S. Rani, and V. Kumar, "Role-Based Access Control (RBAC) Enabled Secure and Efficient Data Processing Framework for IoT Networks," *Int. J. Commun. Networks Inf. Secur.*, Aug. 2024, doi: 10.17762/ijcnis.v16i2.6697.
 31. D. Servos and S. Osborn, "Current Research and Open Problems in Attribute-Based Access Control," *ACM Comput. Surv.*, vol. 49, 2017, doi: 10.1145/3007204.
 32. S. Kosunalp and S. Acik, "Medium Access Control Layer for Internet of Things Edge-Side Network Using Carrier-Sense Multiple Access Protocol," *Eng. Proc.*, vol. 70, no. 1, 2024, doi: 10.3390/engproc2024070001.
 33. T. Ali, M. Al-Khalidi, and R. Al-Zaidi, "Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review," *J. Comput. Inf. Syst.*, vol. 66, no. 1, pp. 123–150, Jan. 2026, doi: 10.1080/08874417.2024.2329985.
 34. P. Pandey, "AI-Enabled Multi-Factor Authentication (MFA) Systems for Private and Public Cloud Security," in 2025 International Conference on

- Electronics and Renewable Systems (ICEARS),
IEEE, Feb. 2025, pp. 886–889. doi:
10.1109/ICEARS64219.2025.10941462.
35. M. Z. Khan, K. U. Nisa, M. T. Quasim, M. A. Khalifa, and M. M. Mobarak, "Cloud-based Data Protection: A Framework for Authorizing Data Movement," in 2024 International Conference on Expert Clouds and Applications (ICOECA), IEEE, Apr. 2024, pp. 271–275. doi: 10.1109/ICOECA62351.2024.00057.
36. Z. Cheng, X. Ding, H. Wan, and K. Liu, "Application and Practice of Data Authorization and Access Technology in Multi-tenant Environment," in 2024 9th International Symposium on Computer and Information Processing Technology (ISCIPT), IEEE, May 2024, pp. 251–255. doi: 10.1109/ISCIPT61983.2024.10673271.
37. R. Khedkar, A. Pawar, K. Dharmale, N. Gaikwad, and A. Kangane, "A Comprehensive Survey of Graphical Passwords Authentication Systems that Provides Security," in 2024 International Conference on Expert Clouds and Applications (ICOECA), IEEE, Apr. 2024, pp. 130–136. doi: 10.1109/ICOECA62351.2024.00036.
38. N. Li, X. Li, Y. Yan, Q. Sun, Y. Han, and K. Cheng, "Joint Communication and Computing Resource Optimization for Collaborative AI Inference in Mobile Networks," in 2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall), IEEE, Oct. 2023, pp. 1–5. doi: 10.1109/VTC2023-Fall60731.2023.10333702.