International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A Critical Review of Cloud Infrastructure Security Using Multi-Factor Authentication

Preethi Patel H G

Department of Computer Science, Sahyadri Science College, Shivamogga, Karnataka, India

Abstract

Cloud computing has become widely adopted due to its ability to provide scalable, flexible, and on-demand services for data storage, application hosting, and online collaboration. However, the security of user accounts and sensitive data remains a significant concern because cloud services are accessed via the internet. Password-based authentication alone is no longer considered sufficient, as passwords may be stolen, guessed, or compromised through phishing, brute-force, replay, and other malicious attacks. In response to these risks, Multi-Factor Authentication (MFA) is employed to strengthen user verification by requiring two or more independent authentication factors. These factors typically include knowledge-based elements, such as passwords or PINs, possession-based elements, such as mobile phones, smart cards, or security tokens, and inherence-based elements, such as fingerprints or facial recognition. This survey examines recent developments in MFA for cloud computing and discusses a range of authentication techniques, including one-time passwords, biometric authentication, smart cards, hardware tokens, mobile-based authentication, and AI-based adaptive authentication systems designed to enhance cloud security It further examines multi-layer security approaches that integrate contextual verification, encryption, access control, and intrusion detection to enhance cloud protection. In addition, this survey discusses the design principles of secure MFA protocols, identifies existing vulnerabilities and implementation challenges, and evaluates recent research trends in deep learning-based authentication and biometric security. Finally, the paper highlights current limitations, emerging technologies, and future research directions toward developing secure, scalable, user-friendly, and privacy-preserving authentication frameworks for next-generation cloud computing environments.

Keywords: Cloud Computing, Multi-Factor Authentication (MFA), Cloud Security, Authentication, Access Control, Biometric Authentication, Identity Management, Authentication Protocols, Intrusion Detection, Deep Learning.

1. Introduction

Cloud computing has become an essential technology for the provision of scalable, on-demand computing resources, allowing organizations and individuals to access storage, applications, and computational services remotely via the Internet**.** Its flexibility, cost-effectiveness, and resource-sharing capabilities have accelerated its adoption across sectors such as healthcare, finance, education, government, and e-commerce. Despite these advantages, the distributed and remotely accessible nature of cloud computing introduces significant security challenges, among which authentication remains one of the most critical. Authentication serves as the first line of defense by verifying the identity of users

before granting access to cloud resources, thereby protecting sensitive data, applications, and administrative services from unauthorized access.

MFA is a good way to make password-only login safer. It uses two or more different checks, such as a password or PIN, a smart card, mobile device, or one-time password, and biometric features like a fingerprint, face recognition, or iris scan. This makes it much harder for unauthorized users to get access, even if one check is stolen or broken. Recent research has further extended MFA through adaptive and multi-layer authentication frameworks that integrate contextual information, such as device identity, reallocation, browser verification, user behavior, access control, intrusion detection systems, and encryption techniques to provide comprehensive protection for cloud environments

Although MFA offers substantial security improvements, recent studies demonstrate that its effectiveness depends not only on the number of authentication factors but also on the design and implementation of authentication protocols. Weak protocol design, improper factor binding, inadequate privacy protection, and incomplete threat models can introduce vulnerabilities that attackers may exploit. Furthermore, the rapid advancement of artificial intelligence and deep learning has enabled significant improvements in biometric authentication systems, while secure hardware technologies, including smart cards, trusted platform modules, and secure enclaves, have strengthened identity verification and cryptographic protection.

This Review Literature provides a comprehensive growth in multifactor authentications for secure cloud computing. . It examines various authentication techniques, analyzes existing authentication frameworks and security threats, compares current approaches based on their strengths and limitations, and discusses practical implementation challenges. Additionally, the survey highlights emerging technologies, including AI-driven authentication, behavioral biometrics, password less authentication, and Zero Trust security models, while identifying future research opportunities for developing secure, scalable, privacy-preserving, and user-friendly authentication frameworks for next-generation cloud computing environments.

2. Background

The Important part of cloud Security is Authentication. It checks whether a user device or application is allowed to access cloud services before permission is given The primary defense layer against unauthorized access is the cloud security and works closely with identity management, authorization, and access control to establish a trusted relationship between cloud service providers and users. As cloud computing has become the backbone of modern digital services, ensuring secure and reliable authentication has become increasingly important for protecting sensitive information, maintaining data integrity, and preserving user privacy.

Unlike traditional computing environments, cloud systems operate across distributed infrastructures and support access from multiple devices, locations, and networks. Users frequently connect to cloud services through laptops, smart phones, web browsers, APIs, and Internet-enabled devices across public, private, and hybrid cloud environments. This flexibility significantly improves accessibility and productivity but also increases the complexity of identity verification. Consequently, cloud authentication mechanisms must be scalable, reliable, user-friendly, and resilient against evolving cyber threats while supporting a large number of users and services.

Budget friendly and simplicity are the main reason are for widely adoption of conventional password based authentication despite this, password alone are no longer sufficient to protect modern cloud

environments because they are susceptible to phishing attacks, credential theft, brute-force attacks, replay attacks, password reuse, and social engineering. These limitations have encouraged researchers and industry practitioners to develop stronger authentication mechanisms capable of providing higher levels of security without significantly affecting user convenience.

To improve cloud security, Multi-Factor Authentication (MFA) is used to provide an extra level of protection during user login. It confirms a user's identity by using more than one verification method. These methods can include information known by the user, such as a password or PIN, items owned by the user, such as a mobile phone, smart card, or security token, and personal characteristics of the user, such as fingerprints, facial features, iris scans, or voice patterns. Using multiple verification steps makes it difficult for attackers to gain access, even if one method is stolen or compromised. Advanced MFA systems also use additional security features like device checking, user activity monitoring, location verification, and adaptive security controls to provide safer access to cloud services.

Recent research has expanded the concept of MFA by introducing multi-layer authentication frameworks that integrate authentication with access control, identity management, session monitoring, and intrusion detection systems. These frameworks continuously evaluate user activities before and after login, enabling the detection of suspicious behavior throughout an active session. Context-aware authentication has also gained significant attention by incorporating additional information such as Geolocation, browser identity, device fingerprints, login history, network characteristics, and user behavior to strengthen identity verification and minimize impersonation attacks. Encryption algorithms such as AES are used to keep login information and communication secure, which helps prevent data exposure during the authentication process.

Although MFA significantly improves security compared to single-factor authentication, its effectiveness depends on the correctness of protocol design and implementation rather than simply increasing the number of authentication factors. Weak protocol construction, improper factor binding, insufficient freshness verification, inadequate privacy protection, or incomplete threat modeling can still expose cloud systems to sophisticated attacks. Therefore, secure authentication requires carefully designed protocols that ensure confidentiality, integrity, availability, and resistance to emerging cyber threats.

Artificial intelligence (AI) and deep learning have improved cloud authentication systems by making biometric identification more accurate and secure. These technologies help systems recognize user features, identify fake attempts, and improve their performance over time. Deep learning methods are commonly used in biometric authentication methods such as face recognition, fingerprint scanning, iris recognition, and voice authentication. In addition, secure hardware technologies—including smart cards, Trusted Platform Modules (TPMs), Near Field Communication (NFC)-based credentials, secure enclaves and hardware security modules—provide secure storage of cryptographic keys and biometric templates. The integration of AI-driven biometrics with secure hardware has led to hybrid authentication architectures that offer stronger protection, improved usability, and enhanced resilience against sophisticated cyberattacks. These developments provide the foundation for modern cloud authentication systems and motivate continued research toward secure, scalable, intelligent, and privacy-preserving authentication frameworks for next-generation cloud computing environments.

3. Literature Review

Cloud computing has become an important technology that allows organizations to access computing

services through the Internet without managing physical infrastructure. It provides advantages such as easy resource sharing, flexible usage, and the ability to increase or decrease services based on requirements. As more sectors, including healthcare, finance, education, government, and online businesses, are adopting cloud platforms, protecting user information and cloud resources has become a major security challenge. Authentication is an essential security step that helps verify users and prevent unauthorized access to cloud systems**.** Over the past two decades, authentication techniques have evolved from traditional password-based mechanisms to sophisticated Multi-Factor Authentication (MFA) frameworks that combine multiple authentication factors and adaptive security mechanisms. The literature demonstrates that although numerous authentication techniques have been proposed, no single approach is capable of addressing all cloud security challenges while simultaneously maintaining usability, scalability, privacy, and implementation efficiency.

In the early stages, authentication systems mainly used a single security method based on usernames and passwords. These systems were easy to set up, required less infrastructure, and were affordable for organizations to implement. However, studies showed that password-based authentication has several security problems. Passwords can be compromised through attacks such as password guessing, phishing, malware, and data breaches. Many users also use simple passwords or the same password for multiple accounts, which increases the possibility of unauthorized access. Due to these limitations, researchers started developing stronger authentication methods that can provide better security while remaining easy for users to operate.

To overcome the shortcomings of password-only authentication, researchers introduced Multi-Factor Authentication (MFA), which verifies user identity using two or more independent authentication factors. Multi-Factor Authentication (MFA) uses different types of verification methods to confirm a user's identity. These methods are mainly divided into three categories: something the user knows, such as a password or PIN; something the user has, such as a smart card, security token, mobile phone, or one-time password; and something the user is, such as a fingerprint, face recognition, iris scan, or voice recognition. The literature consistently reports that combining multiple authentication factors substantially improves security because compromising one factor alone is insufficient to gain unauthorized access. Consequently, MFA has become one of the most widely recommended security mechanisms for protecting cloud infrastructures.

One of the most comprehensive contributions to this field is the systematic survey of Multi-Factor Authentication for cloud infrastructure published in 2023. This work provides a detailed overview of cloud authentication principles, authentication factors, cloud-specific security threats, and recent developments in MFA techniques. The authors classify authentication approaches according to the three fundamental authentication factors and compare their strengths, limitations, and applicability in different cloud environments. Password-based authentication remains attractive because of its simplicity and widespread adoption; however, the survey highlights its inability to withstand modern cyberattacks when used alone. The survey further examines one-time passwords (OTPs), biometric authentication, smart cards, cryptographic tokens, and hybrid authentication methods, emphasizing that each technique offers unique advantages while introducing practical trade-offs related to cost, privacy, usability, deployment complexity, and scalability.

OTP-based authentication has emerged as one of the most commonly deployed second authentication factors in cloud services. The literature indicates that OTP mechanisms significantly improve security by generating temporary authentication codes that expire after a short period. These codes are typically

delivered through SMS, email, authenticator applications, or hardware tokens. OTP-based systems effectively reduce the risk associated with stolen passwords because attackers require both the password and the temporary verification code to gain access. Nevertheless, previous studies have identified several limitations, including SIM-swapping attacks, SMS interception, phishing attacks targeting OTPs, and dependency on network availability. Consequently, researchers increasingly recommend replacing SMS-based OTPs with application-based authenticators or hardware security keys.

Biometric authentication has become an important security method because it identifies users based on their unique physical or behavioral features. Common biometric techniques used in cloud applications include fingerprint scanning, face recognition, iris identification, voice verification, palm vein recognition, and analysis of user behavior patterns. Compared to passwords, biometric characteristics are more difficult to steal or replicate, improving both security and user convenience. However, the literature identifies several challenges associated with biometric authentication, including template protection, privacy concerns, spoofing attacks, sensor reliability, computational requirements, and regulatory compliance. Researchers therefore continue investigating methods for securely storing biometric templates while maintaining high authentication accuracy.

Possession-based authentication methods, including smart cards, USB tokens, cryptographic hardware devices, and mobile authenticators, have also become important components of modern MFA systems. These approaches provide additional security by requiring users to possess physical authentication devices that store cryptographic credentials securely. Smart cards are particularly attractive because they support secure key storage, cryptographic processing, digital certificates, and biometric integration. Despite these advantages, the literature notes that hardware deployment increases implementation costs, introduces management overhead, and requires secure device provisioning and replacement procedures.

Recent studies have shifted beyond traditional MFA toward adaptive and multi-layer authentication frameworks that incorporate contextual information and continuous security monitoring. Instead of verifying user identity only during login, these frameworks continuously evaluate user behavior throughout an active session. Authentication decisions may consider contextual attributes such as geographic location, browser identity, operating system, device fingerprints, IP addresses, login history, network characteristics, and behavioral patterns. Such adaptive authentication mechanisms improve resilience against account hijacking, session theft, insider attacks, and unauthorized privilege escalation. Several researchers have proposed integrating authentication with access control mechanisms, intrusion detection systems, and encryption technologies to provide layered cloud security rather than relying exclusively on login credentials.

The concept of multi-layer authentication has attracted increasing attention because cloud security extends beyond identity verification. One important contribution proposes an authentication architecture that integrates Multi-Factor Authentication with access control, intrusion detection, contextual verification, and AES-based encryption. Unlike conventional authentication systems that terminate security evaluation after successful login, this framework continuously monitors user activities and enforces security policies throughout the session. Context-aware authentication further strengthens identity verification by validating browser characteristics, geographic location, user behavior, and device information before granting or maintaining access. Such approaches significantly reduce opportunities for attackers to exploit compromised credentials after authentication has been completed.

Although MFA is generally considered more secure than single-factor authentication, recent literature demonstrates that protocol correctness is equally important. Merely combining multiple authentication

factors does not guarantee security if the underlying protocol contains design flaws or implementation weaknesses. The ACM Computing Surveys review published in 2025 presents one of the most comprehensive analyses of MFA protocol security. Rather than evaluating authentication methods solely based on the number of authentication factors employed, the study introduces structured evaluation criteria for assessing protocol correctness, privacy protection, freshness verification, factor binding, and resistance to multiple attack models. The authors demonstrate that many published MFA protocols contain previously undiscovered vulnerabilities despite claiming strong security properties.

This systematic evaluation reveals several common weaknesses, including replay attacks, incorrect factor binding, insufficient mutual authentication, weak privacy preservation, inadequate session management, and unrealistic assumptions regarding attacker capabilities. The study emphasizes that authentication protocols should be evaluated using comprehensive threat models rather than theoretical security claims alone. These findings have significantly influenced recent authentication research by encouraging formal protocol verification, rigorous security analysis, and performance evaluation alongside usability considerations

Recent Research as Shown that Artificial Intelligence and deep Learning are playing the major Role in cloud Authentication System. Earlier biometric systems relied heavily on handcrafted feature extraction techniques that often struggled under varying environmental conditions. Recent advances in deep learning have substantially improved biometric recognition accuracy by enabling automatic feature extraction, adaptive learning, spoof detection, and improved generalization across diverse Collection data. The recurrent neural networks, Convolution Neural Networks (CNNs), transformer-based architectures, and multimodal learning techniques have all contributed to improved biometric authentication performance.

The recent survey on deep learning-based Multi-Factor Authentication further expands this research area by examining the integration of artificial intelligence, biometric recognition, and secures hardware technologies between 2019 and 2025. The survey reviews multiple biometric modalities, including facial recognition, fingerprint authentication, iris recognition, and voice authentication, while also discussing hardware-assisted authentication through smart cards, Trusted Platform Modules (TPMs), Near Field Communication (NFC), secure enclaves, and hardware security modules. The study highlights that combining AI-driven biometrics with hardware-based authentication significantly improves authentication robustness while protecting cryptographic keys and sensitive biometric templates.

Despite substantial progress, the literature consistently identifies several unresolved challenges. One of the most significant issues involves balancing security with usability. Highly secure authentication mechanisms may increase login complexity, reduce user acceptance, or introduce accessibility barriers for certain users. Similarly, advanced biometric systems often require specialized hardware, increasing deployment costs for cloud providers. Privacy preservation also remains an important concern because biometric information is permanent and cannot be easily replaced if compromised. Researchers continue exploring privacy-preserving biometric templates, federated identity management, homomorphic encryption, secure multi-party computation, and decentralized authentication mechanisms to address these concerns.

Another recurring theme throughout the literature is the absence of a universally optimal authentication solution. Cloud environments differ significantly in their security requirements, performance expectations, regulatory obligations, and deployment constraints. Consequently, authentication frameworks must be tailored according to application requirements, organizational policies, user

populations, and threat models. Modern cloud security therefore increasingly adopts adaptive authentication.

4. Types of Multi-Factor Authentication

Multi-Factor Authentication (MFA) is one of the most effective security mechanisms for protecting cloud computing environments from unauthorized access. Unlike traditional password-based authentication, MFA requires users to verify their identity using two or more independent authentication factors. These factors are generally categorized into knowledge-based, possession-based, inherence-based, and contextual authentication factors. Modern cloud security systems also employ hybrid authentication schemes that combine multiple techniques to enhance security while maintaining usability.

4.1 Knowledge-Based Authentication

Knowledge-based authentication verifies a user's identity using information that only the legitimate user should know. Common examples include passwords, Personal Identification Numbers (PINs), and answers to security questions. Due to its simplicity and ease of implementation, this remains the most widely used authentication method in cloud computing. However, knowledge-based authentication alone provides limited security because passwords are vulnerable to phishing attacks, brute-force attacks, dictionary attacks, credential theft, password reuse, and social engineering. Consequently, it is rarely recommended as a standalone authentication mechanism in modern cloud environments.

4.2 Possession-Based Authentication

Possession-based authentication requires users to prove ownership of a physical or virtual authentication device. Examples include smart phones, smart cards, USB security keys, hardware tokens, software tokens, and One-Time Password (OTP) generators. Since attackers must possess both the user's credentials and the authentication device, this approach significantly strengthens cloud security. Nevertheless, possession-based authentication may still be compromised through device theft, SIM-swapping attacks, malware infections, cloning attacks, or token synchronization failures. Therefore, additional security mechanisms are often integrated with possession-based authentication.

4.3 Inherence-Based Authentication

Inherence-based authentication relies on unique biological or behavioral characteristics to verify user identity. Common biometric techniques include fingerprint recognition, facial recognition, iris scanning, voice recognition, palm vein recognition, and behavioral biometrics. Biometric authentication offers improved user convenience because users cannot easily forget or lose their biometric characteristics. Furthermore, biometric identifiers are generally more difficult to duplicate than passwords. However, biometric systems introduce important challenges, including privacy protection, secure storage of biometric templates, spoofing attacks, sensor reliability, and regulatory compliance. Once biometric information is compromised, it cannot be easily replaced, making template security a major research concern.

4.4 Context-Based Authentication

Context-based authentication enhances traditional MFA by analyzing additional information related to the user's environment and behavior during the authentication process. Instead of relying solely on credentials, the system evaluates contextual attributes such as geographical location, browser identity, device fingerprint, IP address, login time, operating system, network characteristics, and previous login behavior. If unusual activity is detected, the authentication system may request additional verification

before granting access. Context-aware authentication enables adaptive security and significantly improves the detection of suspicious login attempts, account hijacking, and unauthorized access.

4.5 Password and One-Time Password (OTP) Authentication

Password combined with One-Time Password (OTP) authentication is one of the most widely implemented MFA techniques in cloud computing. In this approach, the password represents the knowledge factor, while the OTP represents the possession factor. OTPs are typically generated through authenticator applications, SMS messages, email verification, or hardware tokens. Since each OTP is valid only for a short period, the technique significantly reduces the risk associated with stolen passwords. However, SMS-based OTP systems remain vulnerable to SIM-swapping attacks, phishing, and message interception. As a result, recent studies recommend application-based authenticators or hardware security keys as more secure alternatives.

4.6 Smart Card Authentication

Smart card authentication employs physical cards containing secure cryptographic credentials to verify user identity. These cards securely store encryption keys, digital certificates, and authentication information within tamper-resistant hardware. Smart cards provide strong possession-based authentication and are widely used in enterprise environments, banking systems, healthcare, and government organizations. Although they significantly improve authentication security, smart cards require specialized hardware, secure distribution, maintenance, and replacement procedures, increasing deployment costs and operational complexity.

4.7 Token-Based Authentication

Token-based authentication uses either hardware or software tokens to generate dynamic authentication codes or cryptographically sign authentication requests. Hardware tokens include USB security keys and dedicated authentication devices, while software tokens are commonly implemented through mobile authentication applications. Token-based authentication is highly effective in protecting enterprise cloud systems because authentication codes continuously change and cannot be reused by attackers. However, token loss, synchronization issues, malware attacks, and device theft remain important operational concerns.

4.8 Hybrid Multi-Factor Authentication

Hybrid MFA combines two or more authentication techniques to provide stronger identity verification than any single authentication method alone. A typical hybrid authentication framework may integrate passwords, OTPs, biometric verification, smart cards, hardware tokens, and contextual authentication. Recent cloud authentication frameworks further incorporate access control, intrusion detection systems, encryption, and continuous session monitoring to establish multiple layers of defense. These adaptive authentication architectures significantly improve resistance against phishing, replay attacks, credential theft, insider attacks, and session hijacking. However, increasing the complexity of authentication protocols also introduces implementation challenges and potential security vulnerabilities if protocols are not carefully designed, formally verified, and regularly updated.

Overall, the literature indicates that no individual authentication factor can provide complete protection for cloud environments. Instead, secure cloud systems increasingly rely on hybrid and context-aware Multi-Factor Authentication frameworks that combine multiple authentication factors with intelligent security mechanisms. Future authentication solutions are expected to integrate artificial intelligence, behavioral biometrics, password less authentication, Zero Trust security principles, and continuous

authentication techniques to provide secure, scalable, user-friendly, and privacy-preserving access control for next-generation cloud computing environments.

5. Cloud Security Threats

Cloud computing has transformed the way organizations store, process, and access information by providing scalable and on-demand services over the Internet. Despite these advantages, the remote accessibility and distributed nature of cloud environments expose authentication systems to a wide range of security threats. Since authentication serves as the primary gateway to cloud resources, any weakness in the authentication process can allow attackers to gain unauthorized access to sensitive data, applications, and services. Consequently, protecting authentication mechanisms has become one of the most important challenges in cloud security.

One of the most common threats to cloud authentication is **phishing**, where attackers deceive users into revealing their login credentials through fraudulent websites, emails, or messages that closely resemble legitimate cloud service providers. Once credentials are stolen, attackers can impersonate legitimate users and gain unauthorized access to cloud accounts. Although Multi-Factor Authentication (MFA) significantly reduces the effectiveness of phishing attacks by requiring additional verification factors, sophisticated phishing campaigns can still target one-time passwords (OTPs), authentication tokens, or biometric verification processes.

Credential theft remains another major security concern in cloud environments. User credentials may be compromised through malware, key loggers, password reuse, database breaches, or social engineering attacks. Since many users continue to reuse passwords across multiple online services, attackers often exploit leaked credentials from one platform to access cloud services. Integrating multiple authentication factors, secure password management, and continuous authentication mechanisms can significantly reduce the impact of credential theft.

Brute-force and dictionary attacks are frequently used to compromise weak or predictable passwords. Automated software repeatedly attempts different password combinations until the correct credentials are discovered. Organizations can reduce these attacks by implementing strong password policies, account lockout mechanisms, rate limiting, CAPTCHA verification, and Multi-Factor Authentication. However, password-only authentication remains vulnerable if users select weak passwords or fail to follow secure password management practices.

Another significant threat is the **replay attack**, in which attackers capture valid authentication messages and retransmit them to gain unauthorized access. Authentication protocols that lack proper freshness verification, timestamp validation, or cryptographic protection are particularly vulnerable to replay attacks. Modern authentication frameworks mitigate these risks through encrypted communication, nonce-based authentication, secure session management, and time-sensitive authentication tokens.

Session hijacking is another serious security issue in cloud computing. Even after successful authentication, attackers may steal or manipulate active session tokens to impersonate legitimate users without requiring additional login credentials. Weak session management, insecure cookies, or insufficient encryption increase the likelihood of session hijacking attacks. Continuous authentication, secure session monitoring, and periodic revalidation of user identity are effective strategies for mitigating these risks.

Cloud environments are also vulnerable to **insider threats**, where authorized users intentionally or unintentionally misuse their privileges. Employees, administrators, contractors, or third-party service

providers may access sensitive cloud resources beyond their authorized responsibilities. Implementing role-based access control (RBAC), least-privilege principles, continuous auditing, and behavioral monitoring can help reduce the risks associated with insider misuse.

Modern cloud authentication frameworks increasingly rely on **context-aware authentication** to strengthen identity verification. Contextual information such as geographical location, browser identity, IP address, device fingerprint, login history, and user behavior is analyzed to determine whether an access request is legitimate. While context-aware authentication significantly improves security, attackers may still attempt to spoof device information, manipulate location data, or imitate legitimate user behavior. Therefore, contextual verification should be combined with other authentication factors to provide stronger protection.

The increasing adoption of **biometric authentication** introduces additional security and privacy challenges. Although fingerprints, facial recognition, iris scans, and voice recognition provide stronger identity verification than passwords, biometric systems remain vulnerable to presentation attacks, spoofing, template theft, and privacy leakage. Since biometric characteristics cannot easily be replaced once compromised, protecting biometric templates through encryption, secure storage, and privacy-preserving techniques has become a critical research area.

Recent advancements in **artificial intelligence and deep learning** have improved the accuracy of biometric authentication systems while introducing new security risks. Deep learning-based authentication systems may be exposed to adversarial attacks, model inversion attacks, data poisoning, and synthetic biometric generation, where attackers manipulate machine learning models to bypass authentication or reconstruct sensitive biometric information. Protecting AI-based authentication systems therefore requires robust model training, adversarial defense mechanisms, secure data handling, and continuous model evaluation.

Possession-based authentication mechanisms, including **smart cards, hardware tokens, USB security keys, and mobile authenticators**, also face security challenges. Physical devices may be lost, stolen, cloned, or damaged, allowing attackers to misuse authentication credentials if additional security measures are absent. Secure cryptographic storage, tamper-resistant hardware, and rapid credential revocation mechanisms are essential for protecting possession-based authentication systems.

Another important concern in cloud environments is **identity federation and trust management**. Many organizations use federated identity services to allow users to access multiple cloud applications using a single identity provider. While federation improves usability and reduces password management complexity, weaknesses in trust relationships, identity providers, or authentication protocols can allow attackers to compromise multiple cloud services simultaneously. Consequently, secure federation protocols, continuous trust verification, and robust identity management frameworks are essential for maintaining secure cloud ecosystems.

Overall, the literature indicates that cloud authentication faces numerous evolving threats that cannot be addressed by a single security mechanism. Modern cloud environments require layered and adaptive security strategies that combine Multi-Factor Authentication, encryption, access control, continuous monitoring, intrusion detection, behavioral analysis, and artificial intelligence to provide comprehensive protection. As cyber threats continue to evolve, future cloud authentication systems must prioritize security, privacy, scalability, and usability while remaining resilient against emerging attack techniques and increasingly sophisticated adversaries.

6. Challenges

Despite the significant advancements in Multi-Factor Authentication (MFA), several challenges continue to hinder its effective deployment in cloud computing environments. As cloud services become increasingly distributed, dynamic, and accessible from multiple devices and locations, designing an authentication framework that simultaneously provides high security, usability, scalability, privacy, and cost-effectiveness remains a complex task. The existing literature indicates that no single authentication mechanism can satisfy all security and operational requirements, making the development of robust cloud authentication systems an ongoing research challenge.

One of the most critical challenges is achieving an appropriate balance between **security and usability**. Strong authentication mechanisms generally require multiple verification steps, which improve protection against cyberattacks but may increase login complexity and reduce user convenience. When authentication procedures become excessively complicated, users may adopt insecure practices such as password reuse, disabling security features, or attempting to bypass authentication requirements. Conversely, authentication mechanisms that prioritize convenience over security may become vulnerable to phishing, brute-force attacks, credential theft, and unauthorized access. Therefore, modern cloud authentication systems must provide strong security while maintaining a simple and user-friendly experience.

Another significant challenge is **scalability**. Cloud computing platforms support millions of users, devices, and applications that require simultaneous authentication with minimal delay. Authentication frameworks must therefore process large numbers of authentication requests efficiently without creating bottlenecks or degrading system performance. As organizations continue migrating large-scale services to the cloud, maintaining low authentication latency while preserving high security remains an important design objective.

Protocol design and implementation also represent major challenges in Multi-Factor Authentication. Recent research demonstrates that simply combining multiple authentication factors does not automatically guarantee security. Authentication protocols must securely bind knowledge-based, possession-based, and inherence-based factors to the same user session while ensuring confidentiality, integrity, freshness, and mutual authentication. Weak protocol design, improper factor binding, inadequate session management, and incomplete threat modeling may introduce vulnerabilities that attackers can exploit through replay attacks, impersonation attacks, session hijacking, or credential misuse. Consequently, authentication protocols require rigorous security analysis, formal verification, and continuous evaluation before deployment.

Another important challenge involves **privacy protection**, particularly in authentication systems that utilize biometric information and contextual user data. Biometric identifiers such as fingerprints, facial images, iris patterns, and voice characteristics represent permanent personal information that cannot easily be changed once compromised. Similarly, contextual authentication mechanisms frequently collect sensitive information, including geographic location, device fingerprints, browser characteristics, login history, and behavioral patterns. Improper handling of this information may expose users to privacy breaches or unauthorized profiling. Therefore, secure storage, encryption, anonymization, and privacy-preserving authentication techniques are essential for protecting user information.

The increasing adoption of **context-aware authentication** introduces additional operational challenges. Authentication systems frequently evaluate contextual attributes such as user location, network characteristics, browser information, and device identity to determine authentication risk. However,

legitimate changes in travel, mobile device usage, software updates, or network connectivity may generate false alarms that incorrectly classify genuine users as suspicious. Excessive false positives may reduce user satisfaction and increase authentication delays, requiring intelligent adaptive mechanisms capable of distinguishing between legitimate behavioral changes and malicious activities.

Another challenge is the **integration of multiple security components** within cloud authentication frameworks. Modern authentication architectures increasingly combine Multi-Factor Authentication with identity management, access control, encryption, intrusion detection systems, continuous monitoring, and behavioral analytics. Although this layered security approach significantly strengthens cloud protection, integrating multiple technologies increases architectural complexity, implementation cost, maintenance requirements, and interoperability challenges. Ensuring seamless communication among these components while maintaining high performance and reliability requires careful system design.

The rapid adoption of **artificial intelligence and deep learning** for biometric authentication introduces new security concerns. Deep learning models have substantially improved biometric recognition accuracy; however, they remain vulnerable to adversarial attacks, model inversion, data poisoning, presentation attacks, and synthetic biometric generation. Attackers may manipulate machine learning models or exploit weaknesses in training datasets to bypass authentication systems. Consequently, developing robust and trustworthy AI-based authentication models remains an important research challenge.

Performance overhead is another practical consideration for cloud authentication systems. Strong authentication mechanisms often require additional cryptographic computations, biometric processing, device verification, or continuous behavioral analysis, which may increase authentication latency and resource consumption. In large-scale cloud environments, excessive computational overhead can reduce service responsiveness and negatively affect the user experience. Authentication frameworks must therefore balance computational efficiency with strong security requirements.

Interoperability also remains an important challenge because cloud services frequently operate across heterogeneous platforms involving multiple cloud providers, identity providers, operating systems, devices, and authentication technologies. Ensuring compatibility among different authentication frameworks while maintaining consistent security policies is essential for supporting secure cross-platform cloud environments. Standardized authentication protocols and federated identity management solutions play a vital role in addressing these interoperability issues.

Furthermore, **credential recovery and device management** continue to present operational difficulties. Users may lose smart phones, hardware tokens, smart cards, or authentication devices, making secure account recovery challenging without weakening authentication security. Designing recovery mechanisms that are both secure and convenient remains a critical requirement for practical cloud authentication systems.

Finally, the literature highlights the need for **standardized evaluation frameworks** capable of consistently measuring the security, performance, privacy, usability, and scalability of Multi-Factor Authentication solutions. Existing studies often employ different datasets, attack models, performance metrics, and evaluation methodologies, making direct comparisons difficult. Establishing common benchmarking standards and realistic testing environments will enable researchers to evaluate authentication frameworks more effectively and accelerate the development of secure, scalable, privacy-

preserving, and user-friendly authentication solutions for next-generation cloud computing environments.

7. Future Research Directions

The rapid evolution of cloud computing and the increasing sophistication of cyber threats continue to drive the development of more secure and intelligent Multi-Factor Authentication (MFA) systems. Although significant progress has been achieved in strengthening cloud authentication, existing research indicates that several important challenges remain unresolved. Future research should therefore focus on developing authentication frameworks that are adaptive, privacy-preserving, scalable, and capable of addressing emerging security threats while maintaining a seamless user experience.

One promising research direction is the development of **adaptive and risk-based authentication** systems. Unlike traditional authentication methods that apply the same level of security to every login attempt, adaptive authentication dynamically adjusts authentication requirements based on contextual information such as user behavior, geographical location, device identity, network characteristics, and assessed risk levels. By requesting additional verification only when suspicious activities are detected, adaptive authentication can improve both security and usability while reducing unnecessary authentication overhead for legitimate users.

Another important area of research is **privacy-preserving authentication**, particularly for biometric and context-aware authentication systems. As biometric technologies become increasingly popular in cloud environments, protecting sensitive biometric templates and personal information has become a critical requirement. Future authentication frameworks should incorporate advanced template protection techniques, secure enclaves, encryption methods, and privacy-preserving machine learning approaches, such as federated learning, to ensure that sensitive user information remains protected throughout the authentication process.

The application of **artificial intelligence and deep learning** is expected to play a significant role in the next generation of cloud authentication systems. Future studies should focus on developing robust deep learning models that are resistant to adversarial attacks, spoofing attempts, model inversion attacks, and data poisoning. Researchers should also investigate multimodal biometric authentication systems that combine multiple biometric characteristics, such as facial recognition, fingerprints, iris recognition, and voice authentication, together with smart cards or hardware security devices to improve authentication accuracy, reliability, and resilience.

Another key research direction involves improving the **security of authentication protocols** through formal verification and rigorous protocol analysis. Future authentication protocols should provide stronger factor binding, secure session management, resistance to replay and phishing attacks, and realistic threat modeling before deployment. Standardized security evaluation frameworks and benchmarking methodologies are also required to enable consistent comparison of authentication solutions across different cloud environments and application domains.

With the rapid growth of mobile computing, Internet of Things (IoT), and edge computing, researchers should also develop **lightweight Multi-Factor Authentication schemes** that provide strong security while minimizing computational complexity, communication overhead, and energy consumption. Such lightweight authentication mechanisms will be essential for resource-constrained devices operating in distributed cloud ecosystems.

Furthermore, future cloud authentication systems should be designed to integrate seamlessly with **Zero Trust security architectures**, where every access request is continuously verified regardless of network location or previous authentication status. Continuous authentication, behavioral monitoring, identity management, access control, and intrusion detection should work together to provide comprehensive protection throughout the user's session rather than only during the initial login process.

In summary, future research should focus on developing intelligent, adaptive, privacy-preserving, and standardized Multi-Factor Authentication frameworks that effectively combine artificial intelligence, biometrics, secure hardware, contextual information, and continuous security monitoring. These advancements will contribute to the development of secure, scalable, user-friendly, and resilient authentication solutions capable of protecting next-generation cloud computing environments against evolving cyber threats.

8. Conclusion

Cloud services are popular because they provide adaptable, scalable, and economical computing for people and organizations. As more applications and data move to the cloud, safeguarding access becomes critical. Relying only on passwords is risky since they can be stolen, guessed, or abused through tactics like phishing, brute-force attacks, replaying credentials, session takeover, or insider misuse. Multi-factor authentication strengthens protection by requiring two or more different proofs of identity (for example, a password plus a device code or a biometric). This layered approach makes it far harder for attackers to gain access even if one credential is exposed.

This survey reviewed recent developments in Multi-Factor Authentication for cloud computing by examining various authentication techniques, including knowledge-based, possession-based, inherence-based, context-aware, token-based, smart card-based, biometric, and hybrid authentication methods. The literature demonstrates that each authentication technique provides unique advantages while also presenting specific limitations related to usability, implementation complexity, scalability, deployment cost, and privacy protection. Therefore, selecting an appropriate authentication mechanism depends on the security requirements, application environment, and user needs of a particular cloud system.

The reviewed studies further demonstrate that effective cloud authentication extends beyond verifying user identity during login. Modern authentication frameworks increasingly integrate access control, continuous monitoring, intrusion detection, contextual verification, encryption, and behavioral analysis to provide comprehensive protection throughout the user's interaction with cloud services. Recent advancements in artificial intelligence and deep learning have also enhanced biometric authentication by improving recognition accuracy, adaptive decision-making, and attack detection. At the same time, secure hardware technologies such as smart cards, Trusted Platform Modules (TPMs), and secure enclaves have strengthened possession-based authentication and protected sensitive cryptographic information.

Despite these significant advancements, several challenges remain unresolved. Balancing security with usability, preserving user privacy, ensuring protocol correctness, supporting interoperability across heterogeneous cloud environments, and maintaining high performance under large-scale deployments continue to be major research concerns. Furthermore, emerging threats targeting authentication protocols, biometric systems, and AI-based authentication models highlight the need for continuous security evaluation and protocol improvement.

Overall, the findings of this survey indicate that no single authentication technique can provide complete protection for every cloud environment. Future cloud security will increasingly rely on intelligent, adaptive, and privacy-preserving authentication frameworks that combine multiple authentication factors with contextual awareness, artificial intelligence, continuous monitoring, and Zero Trust security principles. Continued research in these areas will contribute to the development of secure, scalable, resilient, and user-friendly authentication systems capable of protecting next-generation cloud computing infrastructures against evolving cyber threats.

References

1. S. P. Otta, S. Panda, M. Gupta, and C. Hota, "A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure," Future Internet, vol. 15, no. 4, Art. no. 146, 2023, doi: 10.3390/fi15040146.
2. M. A. Alghamdi, "Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication," Applied Sciences, vol. 13, no. 19, Art. no. 10871, 2023, doi: 10.3390/app131910871.
3. A. K. Wee, E. G. Chekole, and J. Zhou, "Unveiling the Covert Vulnerabilities in Multi-Factor Authentication Protocols: A Systematic Review and Security Analysis," ACM Computing Surveys, vol. 58, no. 2, 2025, doi: 10.1145/3734864.
4. A. K. Wee, E. G. Chekole, and J. Zhou, "Excavating Vulnerabilities Lurking in Multi-Factor Authentication Protocols: A Systematic Security Analysis," arXiv preprint arXiv:2503.18024, 2025.
5. A. Ganmati, K. Afdel, and L. Koutti, "Deep Learning-Based Multi-Factor Authentication: A Survey of Biometric and Smart Card Integration Approaches," arXiv preprint arXiv:2510.05163, 2025.