



Maximizing Cloud Security: Synergistic Approaches to Multi-factor Authentication Deployment

M.P. Dhanveer Prakash¹ and Anurag Singh^{2*}

^{1,2}School of Computer Science Engineering, Lovely Professional University, Punjab, India

*rax93singh@gmail.com

Abstract. Cloud computing has transformed traditional IT infrastructure, offering dynamic, configurable resources on demand. On the other hand, it brings unique cybersecurity challenges, particularly in protecting sensitive data from unauthorized access. Traditional single factor authentication does not address these risks. By implementing multi-factor authentication (MFA), which combines several factors for verification including password, tokens, and biometrics, this cloud security method has become increasingly popular. Existing authentication methods fall short in the cloud environment, so this paper presents a novel multi-factor, multi-layered cloud access authentication framework. The methodology for MFA implementation uses risk-adaptive authentication based on real-time risk assessment, adaptive policy for MFA selection, and seamless verification workflows for end-users. Moreover, the implementation of the advanced technologies that cover all aspects such as encryption, SSO, and adaptive authentication further safeguards it against evolving threats. Through experimental analyses, we show that the framework is effective to substantially reduce the vulnerabilities without compromising usability and scalability. This will help cloud service providers and organizations alike better equip themselves with an effective and agile security environment through the adoption of next generation MFA strategies.

Keywords: Multi-factor authentication (MFA), SSO, Vulnerability, Encryption.

1 Introduction

Cloud computing has become a disruptive technology in the last few years, offering Internet-enabled services like storage and processing power. Cloud computing is now an essential characteristic of modern IT infrastructure that enables on-demand access to configurable resource. While it has important benefits, this technology also introduces a lot of security risks. One of the largest challenges in cloud computing is maintaining control over data once it is hosted in the cloud. The cloud model does not assure security measures, for instance, privacy and loyalty consequently this makes data in the cloud susceptible to numerous threats. Authentication of data is the first step to information security and protecting it from unauthorized access. Widely used in the cloud, single-factor authentication does not provide nearly enough security. Multi-factor authentication (MFA) necessitates the confirmation of two or more verification factors before an object, like an application, online account or VPN can be

© The Author(s) 2025

S. Bhalerao et al. (eds.), *Proceedings of the International Conference on Recent Advancement and Modernization in Sustainable Intelligent Technologies & Applications (RAMSITA-2025)*, Advances in Intelligent Systems Research 192,

https://doi.org/10.2991/978-94-6463-716-8_70

accessed. This is a part of IAM strategies, identity and access management. MFA reduces the likelihood of cybers by adding layers of verification that are made in addition to a username and password attacks being successful. MFA (multi-factor authentication) is another way to secure the most common attacks because it provides a much stronger type of authentication, which is why MFA continues to gain traction in cloud computing. By designing MFA — the use of more than one verification factor such as passwords, tokens, or biometric data to access a device or application to add multiple layers of security against unauthorized access. However, the actual MFA only would provide a benefit when the attached authentication methods used are strong enough. Various methods for securing cloud resources include Password-based authentication, Biometric authentication, Token-based Authentication, and MFA. A few recent innovations have positioned multiple factor to take in cloud request to secure productivity and complying with regulations. But this only works if you choose the correct authentication factors to use in MFA and do them right.

By offering a variety of authentication options as of Fig.1, the framework (Multi-Factor Authentication with Risk-Adaptive Authentication) aims to provide a comprehensive solution. With this research, gaps in current authentication practices are addressed, and innovative techniques are introduced to strengthen cloud security. As the paper proceeds, it provides valuable insights into enhancing authentication and security in cloud computing environments by describing the framework through the pseudocode..

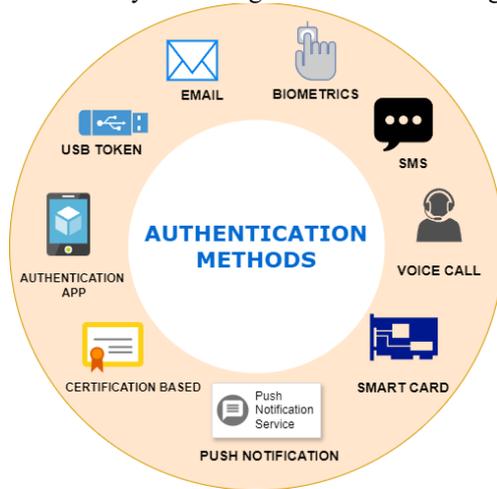


Fig.1. Types of authentication methods

2 Literature Survey

Jayalekshmi Jayakumar and Sr. Mercy Joseph has provided insight into various technologies that are utilized in security architectures, including smart cards, smart phones, OTP tokens, GPS tools, and biometric confirmations, such as fingerprint scanners, iris scanners, or face scanners. The current user authentication system has security flaws, leaving it susceptible to replay, exhaustive, and dictionary attacks despite the advantages of MFA. Additional costs and the management of multiple

passwords are also challenging [1]. For user authentication, proposed security architectures integrate multiple factors such as data, ownership, location, and time to address these shortcomings. As a result, advanced attacks are protected and layered security approaches are ensured for cloud data access [1]. AlsharifHasan Mohamad Aburbeian and Manuel Fernández-Veiga has incorporated authentication technologies such as username-passwords, OTPs, fingerprints, and face recognition, MFA frameworks demonstrated their effectiveness despite customer reluctance and technological constraints in managing large datasets. Further, the integration of machine learning (ML) and multi-factor authentication (MFA) has been identified as a promising way to secure online financial transactions. Evaluation criteria include ML classifier performance and MFA effectiveness metrics, including authentication factors, fraud detection, and e-commerce platforms [2]. A number of advancements in encryption methods, including cipher text-policy attribute-based encryption (CP-ABE), and integration of technologies such as Single Sign-On (SSO), RSA algorithm, and blockchain into MFA frameworks, were discussed, highlighting security risks, privacy concerns, and the need for complexity, usability, and scalability to be addressed [3]. Khalid Mahmood has investigated innovative approaches to enhance the security of MFA, including elliptic curve cryptography (ECC), 5G, Zigbee, and edge computing to address vulnerabilities and ensure user anonymity [4]. Advanced authentication models such as Cloud Shield Architecture (CSA), which combine MFA, behavioral analysis, and machine learning, offer multilayered security through biometrics, OTPs, and hardware tokens [5]. Secure data transfers and three-factor authentication in the cloud have also been explored using encryption algorithms such as SHA-512, CHA, MECC, and CCP, which performed better than existing systems [6]. Additionally, hybrid dynamic encryption addresses security vulnerabilities and ensures efficiency in remote authentication using multi-factor verification [7]. In order to mitigate cloud computing security risks, multi-factor authentication-based frameworks are more important than ever [8]. By integrating secure access service edge (SASE), cloud security posture management (CPSM), and technologies such as Cipher Cloud, cloud data security is enhanced, addressing concerns such as data breaches and denial-of-service attacks [9]. With innovations in authentication mechanisms, such as graphical passwords and behavior-based biometrics, dynamic authentication processes and risk-based approaches are essential [10]. User registration, privilege management, and multi-layer authentication to protect identities are used in the security framework for cloud applications, which allows the robust protection. Using intrusion detection mechanisms, access control policies, and AES threshold encryption guarantee data protection during transmission and storage. It also provides audit and suspected tables to monitor user activities and violations, and achieves high detection accuracy with a low false positive rate [11]. This paper discusses the security issues of EHR in the cloud-based SDN framework and presents a robust three-phase cryptographic authentication scheme that has been verified with the help of AVISPA tool. Also, it proposes a secure Remote Health Monitoring System (RHMS) and a multi-factor authentication protocol to protect against privacy violation and preserve the integrity and originality of data [12]. But because it is unable to self-update, older versions of the multi-factor authentication system will eventually fail to work on modern mobile and desktop operating systems. Also, it's possible that if users work over virtual private networks (VPN), conflicting IP addresses could disrupt their ability to access the system while

employing a software. If they don't have your network available they will struggle to get logged in [13]. IIoT provides excellent and secure multi-factor authentication protocol using symmetric cryptography, hash functions, and XOR operations to achieve authentication, anonymity, untrace ability, forward security, and resistance against replay, man-in-middle, and denial of service attacks. It employs data encryption in the smart card context: It prevents insider users to steal the smart card and calculate corresponding secret credentials. The new user key generation is such that even if an attacker can get the gateway key, he still does not have the important parameter required to derive the user key, and further gain more information. Session-specific temporary information is processed, thereby preventing "leakage" of the session key as a result of its disclosure. Moreover, the user can set up the key with all sensing devices at one-round authentication using a secret sharing scheme [14]. The paper discusses the security proof provisioned by Fotouhi et al. by showing that their scheme, although recently formally proved under ROM model, is vulnerable to three types of attacks, which are offline password guessing attack, user impersonation attack, and de-synchronization attack. The user impersonation attack and de-synchronization attack correspond to the failure [15].

3 Different Types Of MFA In Cloud

Security experts consider MFA an essential component of cloud security. A multi-factor authentication scheme uses multiple authentication factors to verify users' identities, thereby increasing security beyond password-based approaches as mentioned in Table 1. There are different types of MFA, each with unique strengths and security concerns [16].

TABLE 1. Strengths and security issues of different MFA in cloud computing

MFA Type	Strengths	Security Issues
Password-Based Authentication	Cost-effective, and widely supported across various cloud. Platforms and applications.	Phishing, keylogging, man-in-the-middle attacks, brute- force attacks.
Token-Based Authentication	Enhanced security, scalability, and resistance to phishing attacks.	Token interception, Lack of token protection, Token replay attacks, Token expiration vulnerabilities.
Biometric Authentication	High security, convenience, and resistance to credential theft and phishing.	Spoofing, replay attacks, biometric data theft.
One-Time Password (OTP)	Time-sensitive codes, protecting from unauthorized access.	Phishing, interception, replay attacks, device loss, and weak OTP. generation algorithms.
Push Notification Authentication	Convenient, instant, and secure, push notification authentication.	Interception, spoofing, and Device theft vulnerabilities.

Certificate-Based Authentication	Strong security, scalability, and resistance to common attacks like phishing.	Certificate compromise, trust issues, and improper certificate management.
Smart Card Authentication	Portable, and tamper-resistant; provides strong authentication through physical possession.	Theft, loss, and physical tampering risks.
Device Authentication	Reliable, and enhanced security through unique device identifiers.	Unauthorized access, lack of updates, device cloning or replication.
Time-Based Authentication	This authentication offers simplicity, scalability, Increased security. And resistance to common attacks like phishing.	Synchronization errors, Vulnerable to replay attacks, Dependency on accurate system time, Risk of token interception.

4 Security Measures

MFA plays a role in enhancing security in cloud settings where safeguarding data is of utmost importance. This method involves using tactics such as encryption, access restrictions and strong authentication methods and lot more security threats in Fig.2 to keep in mind while working to protect user identities and deter entry [17], [18].



Fig.2. Types of threats on multi factor authentication in cloud

4.1 Encryption

Ensure that authentication data at rest and in transit is encrypted, including user credentials, tokens, and session information. TLS/SSL is used for encryption during transit, and AES is used for encryption during storage. Data integrity and regulatory

compliance can be ensured by utilizing secure key management, end-to-end encryption, and secure communication channels [19].

4.2 **Single Sign-on (SSO)**

When Single Sign On (SSO) is paired with MFA it makes accessing cloud services easier, by directing users to a central authentication portal. Users input their credentials once. Then go through a second verification step like using an OTP. Once the authentication is successful they gain access ensuring a login process, with added security features.

4.3 **Adaptive Authentication**

Dynamic authentication, or for factor authentication (MFA) in the cloud changes its method based on different factors encountered and their level of risk. It assesses user data assigns risk levels and enforces verification methods. Over time decisions are made based on observing behaviour patterns and gaining insights with user engagements. Versioning IAM and SSO integration will boost authentication processes, across cloud environments [20].

4.4 **Multi-Channel Verification**

For Multi-Factor Authentication (MFA) in cloud services, we use communication channels to verify the identity of a user. It integrates channels like email, text messages, phone calls and mobile apps to send verification codes/requests for authentication. By enhancing communication channels, this approach minimizes the risk of unauthorized access by adding multiple confirmation layers to increase security.

4.5 **Identity and Access Management**

Identity and Access Management: authenticating user entry to assets based on their individual characteristics (and obviously, factor authentication (MFA) for cloud services). Includes things like users validation, giving permissions and monitoring privileges. Therefore, IAM tools assure that employees get an appropriate access to the cloud in such a way that the entry of malefactors and data breach would be reduced.

5 **Methodology: Multi-Factor Authentication with Risk-Adaptive Authentication overview**

MFA does work, but its setup also requires some thought. Verification requests are sent to users devices through different communication methods that include push notifications, SMS alerts and authenticator apps among others. These notifications are addressed by the users personally receiving push alerts or entering one time passcodes (OTPs) privately, or accessing time based passwords via authenticator apps. Secondly user interfaces need to display the selected MFA factor so that users can quickly

respond to verification challenges as mentioned in Table 2. The real time validation processes securely transmit user responses to the cloud platform for comparison with expected results. This includes confirming user approval for push notifications matching entered OTPs with generated codes for SMS and authenticator apps or verifying scans against stored data. Additionally following coding practices is crucial in safeguarding against vulnerabilities and ensuring the storage of user credentials and MFA secrets. Lastly integrating with cloud service providers such as AWS Cognito or Azure Active Directory simplifies the incorporation of MFA methods by offering libraries and features, for deployment and management. Table 2. provides the pseudocode framework overview to implement Multi-Factor Authentication with Risk-Adaptive Authentication (MFA-RAA).

5.1 User login and initial authentication

When users log in to a cloud application it is required to enter their login details, a username and password. The credentials are securely transmitted to the cloud platform using HTTPS connections to encrypt the data during transfer. The cloud platform then starts an authentication process by checking the user's identity with a central authentication database. This database, which could be a directory service or an on premise LDAP server verifies users login information, in time.

5.2 Risk Assessment

During log in the cloud platform collects information such as your IP address details about your device, the time of login and your past logins. This helps verify your identity, using the IP for location tracking, checking the device for any access patterns monitoring login times, for irregularities and reviewing login history to spot any potentially suspicious activities.

5.3 MFA Selection and Triggering

The Risk Assessment Module calculates a risk score for each login attempt, which's then cross referenced with thresholds (Low, Medium High) to classify the level of risk. These thresholds establish the distinctions between risk categories. Inform the subsequent steps for multi factor authentication.

Low Risk: When the risk level falls below the threshold it allows immediate access, without requiring a multi factor authentication challenge for familiar login situations.

Medium Risk: If the risk level is between the medium thresholds it will trigger an user friendly factor of multi factor authentication like a push notification or SMS.

High Risk: In cases where the risk level exceeds the threshold it mandates a strong two factor authentication process, such as using a one-time password from an authenticator app and performing a biometric scan.

TABLE 2. Multi-Factor Authentication with Risk-Adaptive Authentication (MFA-RAA)

```

Function CMFA_RA (username, password):
# Initial Authentication
if verify_credentials (username, password) == True:
# Risk Assessment Module
risk_score = assess_risk(user_location (), device_info(),
login_time(), login_history())
# MFA Selection
If risk_score < LOW_RISK_THRESHOLD:
# Grant Login (Low Risk)
return LOGIN_GRANTED
elif risk_score < MEDIUM_RISK_THRESHOLD:
# Single-factor MFA (Medium Risk)
if request_mfa_verification(send_push_notification ()):
return LOGIN_GRANTED
else:
return MFA_FAILED
else:
# Two-factor MFA (High Risk)
if request_mfa_verification(get_otp_from_authenticator ())
AND verify_fingerprint()):
return LOGIN_GRANTED
else:
return MFA_FAILED
else:
return INVALID_CREDENTIALS
Function assess_risk (location, device_info, login_time,
login_history):
risk_score = 0
risk_score += weight_location *
evaluate_location_risk(location)
risk_score += weight_device *
evaluate_device_risk(device_info)
risk_score += weight_time * evaluate_time_risk(login_time)
risk_score += weight_history *
evaluate_history_risk(login_history)
return risk_score

```

```

Function request_mfa_verification(mfa_challenge):
if validation_successful:
return True
else:
return False

```

5.4 MFA Verification

As part of the CMFA-RA system, MFA verification operates in real time, starting with the cloud platform delivering the chosen challenge (push notification, SMS, authenticator app) to the user's registered device. User interactions include approving notifications, entering passcodes, or performing biometric scans. A real-time validation is then performed on the user's response against the expected outcome of the selected MFA factor. If verified the appropriate access is granted if not, error messages are shown or additional security measures taken.

5.5 Authorization

Cloud platforms digitally issue secure session tokens to authorized users after successful completion of their Multi- Factor Authentication (MFA) verification, and allow access to the resources and functionalities of a cloud application. Authorization is denied if the user fails an MFA check (i.e., enters an incorrect passcode or presents a bad fingerprint scan). These situations may cause the system to show an error message on the login screen asking to retry with a MFA challenge, locking-out the account after certain number of failed attempts, and logging that failed attempt for security auditing.

Cloud environments utilize Multi-Factor Authentication (MFA) along with Risk-Adaptive Authentication (RA) in fig.3, allows to assess risk and provide further authentication challenges while performing continuous verification of users. Seamless validation workflows, seamless integrations with cloud- native apps, and an intuitive MFA selection process form a secure authentication framework. And it makes for a very good experience when paired with MFA, and RA creates quick access to cloud resources in a secure manner.

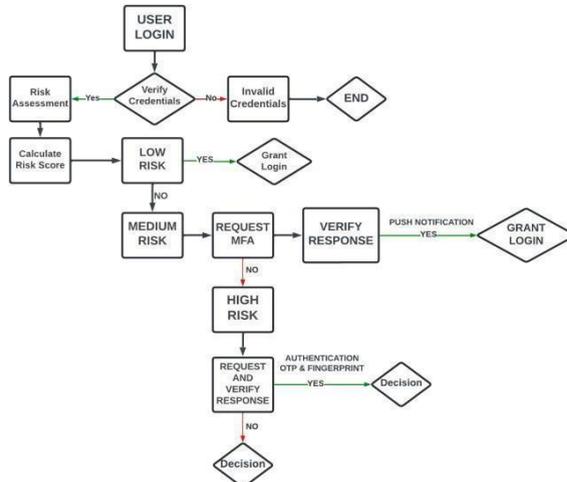


Fig.3. Multi-Factor Authentication with Risk-Adaptive Authentication Flowchart

6 Future Scope

Exploring new MFA factors beyond traditional biometrics, such as behavior-based authentication or context-aware authentication allows us to improve security without sacrificing user experience. The use of new technologies such as blockchain or AI within the MFA mechanism also represents a novel forensic community research opportunity. For example, the scalable and interoperable nature of MFA solutions can allow for once deployment across multiple clouds or domains to enable the ease of management. The human factors in MFA adoption, like user education and awareness as well as usability will also be a must thing to address. Clearly, the future policies and

practices (the road ahead) in the area of Cloud Security will need to delve into the regulation and standardization for MFA adoption/deployment within a Cloud service environment.

7 Conclusion

The topic of Multi factor authentication (MFA) is crucial for enhancing cloud security by introducing additional layers of verification that effectively lower the chances of unauthorized entry, into systems or data breaches. Detailed in this paper is a Multi-Factor Authentication with Risk-Adaptive Authentication framework that aims to overcome the limitations of authentication methods which often rely on single factor approaches and struggle to keep up with emerging cybersecurity risks. This framework integrates elements to provide context aware authentication procedures that can be adjusted based on specific security needs through authentication, risk Assessment, MFA Selection and Triggering, verification and authorization. Moreover, incorporating verification techniques such as scans, OTPs and behavioral analysis improves dependability while still ensuring user convenience. By combining MFA with technologies like encryption Single Sign On (SSO) and adaptive authentication it strengthens security without sacrificing ease of use. This strategy guarantees entry to cloud assets. Reduces the likelihood of exposure, to dangers related to breaches of information and cyber assaults. As more businesses switch to cloud technology, the creation and implementation of MFA solutions will continue to be crucial for ensuring reliable cloud systems. Prioritizing scalability, compatibility among systems and educating users helps maintain the practicality and efficiency of the framework, in real life scenarios.

References

1. Jayakumar, J., Mercy Joseph Assistant Professor Amal Jyothi, S.: Cloud Multi-Factor Authentication. 4., <https://doi.org/10.5281/zenodo.6374810>.
2. Aburbeian, A.H.M., Fernández-Veiga, M.: Secure Internet Financial Transactions: A Framework Integrating Multi-Factor Authentication and Machine Learning. AI (Switzerland). 5, 177–194 (2024). <https://doi.org/10.3390/ai5010010>.
3. Mostafa, A.M., Ezz, M., Elbashir, M.K., Alruily, M., Hamouda, E., Alsarhani, M., Said, W.: Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication. Applied Sciences (Switzerland). 13, (2023). <https://doi.org/10.3390/app131910871>.
4. Mahmood, K., Akram, W., Shafiq, A., Altaf, I., Lodhi, M.A., Islam, S.H.: An enhanced and provably secure multi-factor authentication scheme for Internet-of-Multimedia-Things environments. Computers and Electrical Engineering. 88, (2020). <https://doi.org/10.1016/j.compeleceng.2020.106888>.
5. S. Renuka, Dr.N. Suresh Kumar.:cloud shield architecture: a proposed model for high level authentication”. Journal of research administration: ISSN:1539-1590 | E-ISSN:2573-7104, Vol. 5 No. 2, (2023).
6. Vengala, D.V.K., Kavitha, D., Kumar, A.P.S.: Three factor authentication system with modified ECC based secured data transfer: untrusted cloud environment. Complex and Intelligent Systems. 9, 2915–2928 (2023). <https://doi.org/10.1007/s40747-021-00305-0>.

7. Obaidat, M., Brown, J., Obeidat, S., Rawashdeh, M.: A hybrid dynamic encryption scheme for multi-factor verification: A novel paradigm for remote authentication. *Sensors (Switzerland)*. 20, 1–32 (2020). <https://doi.org/10.3390/s20154212>.
8. Singh, C., Deep Singh, T.: Article ID: IJCET_10_01_020 Cite this Article: Charanjeet Singh and Dr. Tripat Deep Singh, A 3-Level Multifactor Authentication Scheme for Cloud Computing. *International Journal of Computer Engineering & Technology (IJCET)*. 10, 184–195.
9. Suleski, T., Ahmed, M., Yang, W., Wang, E.: A review of multi-factor authentication in the Internet of Healthcare Things, (2023). <https://doi.org/10.1177/20552076231177144>.
10. Manzoor, A., Shah, M.A., Khattak, H.A., Din, I.U., Khan, M.K.: Multi-tier authentication schemes for fog computing: Architecture, security perspective, and challenges. *International Journal of Communication Systems*. 35, (2022). <https://doi.org/10.1002/dac.4033>.
11. Said, W., Mostafa, E., Hassan, M.M., Mostafa, A.M.: A multi-factor authentication-based framework for identity management in cloud applications. *Computers, Materials and Continua*. 71, 3193–3209 (2022). <https://doi.org/10.32604/cmc.2022.023554>.
12. Midha, S., Verma, S., Kavita, Mittal, M., Jhanjhi, N., Masud, M., AlZain, M.A.: A Secure Multi-factor Authentication Protocol for Healthcare Services Using Cloud-based SDN. *Computers, Materials and Continua*. 74, 3711–3726 (2023). <https://doi.org/10.32604/cmc.2023.027992>.
13. Okeke, R.O., Orimadike, S.O.: Enhanced Cloud Computing Security Using Application-Based Multi-Factor Authentication (MFA) for Communication Systems. *European Journal of Electrical Engineering and Computer Science*. 8, 1–8 (2024). <https://doi.org/10.24018/ejece.2024.8.2.593>.
14. Han, Y., Guo, H., Liu, J., Ehui, B.B., Wu, Y., Li, S.: An Enhanced Multifactor Authentication and Key Agreement Protocol in Industrial Internet of Things. *IEEE Internet Things J.* 11, 16243–16254 (2024). <https://doi.org/10.1109/JIOT.2024.3355228>.
15. Wang, Q., Wang, D.: Understanding Failures in Security Proofs of Multi-Factor Authentication for Mobile Devices. *IEEE Transactions on Information Forensics and Security*. 18, 597–612 (2023). <https://doi.org/10.1109/TIFS.2022.3227753>.
16. Hassan, M.A., Shukur, Z.: A Secure Multi Factor User Authentication Framework for Electronic Payment System. In: 2021 3rd International Cyber Resilience Conference, CRC 2021. Institute of Electrical and Electronics Engineers Inc. (2021). <https://doi.org/10.1109/CRC50527.2021.9392564>.
17. Reddy, M.V., Charan, P.S., Devisaran, D., Shankar, R., Kumar, P.M.A.: A Systematic Approach towards Security Concerns in Cloud. In: Proceedings of the 2023 2nd International Conference on Electronics and Renewable Systems, ICEARS 2023. pp. 838–843. Institute of Electrical and Electronics Engineers Inc. (2023). <https://doi.org/10.1109/ICEARS56392.2023.10085437>.
18. Konwar, R., Jha, D., Agrawal, R., Purkayastha, R., Banerjee, I.: A Two-Factor Authentication Mechanism Using a Novel OTP Generation Algorithm for Cloud Applications. In: Proceedings of the 14th International Conference on Cloud Computing, Data Science and Engineering, Confluence 2024. pp. 245–250. Institute of Electrical and Electronics Engineers Inc. (2024). <https://doi.org/10.1109/Confluence60223.2024.10463309>.
19. Mihailescu, M.I., Nita, S.L.: A Searchable Encryption Scheme with Biometric Authentication and Authorization for Cloud Environments. *Cryptography*. 6, (2022). <https://doi.org/10.3390/cryptography6010008>.
20. Mahalakshmi, B., David, B.: An Analytical Survey on Multi-Biometric Authentication System for Enhancing the Security Levels in Cloud Computing. In: Proceedings of 8th IEEE International Conference on Science, Technology, Engineering and Mathematics, ICONSTEM 2023. Institute of Electrical and Electronics Engineers Inc. (2023). <https://doi.org/10.1109/ICONSTEM56934.2023.10142265>.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

