International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

LIGHTWEIGHT AUTHENTICATION MECHANISM FOR MULTI-FACTOR AUTHENTICATION IN MULTI-CLOUD ENVIRONMENT USING ELLIPTIC CURVE CRYPTOGRAPHY

Gandhikota Umamahesh[1*], Dr.G.V.S.Rajkumar[2]

[1a] Research scholar, CSE Department - GITAM University,

Visakhapatnam, Andhra Pradesh, India.

e-mail: mahesh.gandikota@gmail.com

[1b] Assistant Professor, CSE Department - Aditya University,

Surampalem, Andhra Pradesh, India.

e-mail: mahesh.gandikota@gmail.com

[2]Professor, CSE Department - GITAM University,

Visakhapatnam, Andhra Pradesh, India.

e-mail: gganapav@gitam.edu

Abstract

Authentication methods make sure that only the right people can use cloud services. These days, more than one authentication factor is used simultaneously to make authentication stronger. Even if two authentication factors are compromised, the multi-factor authentication (MFA) protocol will still provide the best security available. This paper protects individual privacy when using cloud storage by ensuring anonymity and unlikability. The new thing is that the session key is also safe because each user and cloud server gets a unique session key. Also, the protocol must provide complete privacy and remain safe from attackers if data leaks temporarily. Ability to resist attempts to impersonate another user, server, or even a privileged insider. Utilization of a random model with Elliptic Curve Cryptography (ECC) to test the scheme's strength by showing that important information cannot be taken from messages sent and received during login and authentication. The simulation results indicate that the proposed method reduces the time compared to other existing methods.

Key Words and Phrases: Multi-Factor Authentication, Privacy, Security, Elliptic Curve Cryptography

Introduction

Cloud computing has replaced traditional on-premises data centres as the norm in today's world of widespread internet and communication technology. This platform is helpful because it lets many users share expensive processing power and makes it easy for them to get to big volumes of data whenever they need it [1]. In recent years, ~~a~~ lot of people and enterprises have started using cloud computing since its resources are reliable and available [2]-[4].

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

However, security and privacy problems that might come up when many individuals use cloud services via a public network. It is easy for hackers to read, change, or forge messages sent during a conversation [5].

This makes it hard to guarantee safety in the cloud because there are so many internal and external attackers to these services. For the sake of customer privacy and security, their different cloud accounts must be separate and unrelated [6]. This is especially true when storing sensitive information like medical and financial records in the cloud. Private information includes patient records and financial information. So, trustworthy two-way authentication is necessary [7], [8] to make sure that the user is an authenticated one.

You can use single-factor, two-factor, or multi-factor authentication. Everyone who is involved in the user authentication process knows the passwords that single-factor authentication systems employ. People often fall for password guessing and dictionary attacks since most passwords are short strings of characters. The security researchers came out with two-factor authentication techniques to fix these problems. These systems use both passwords and smart cards to make sure the user is an authenticated user [9]. There are different sorts of authentication factors in Figure 1.

However, this two-factor authentication mechanism can be broken by attacks like stealing a smart card or predicting an password [10]. Biometric traits are being utilised as a backup way to identify people in multi-factor authentication processes. This can assist keep security breaches from happening. There are many benefits of using biometric authentication [11]. This makes it hard to spoof, replicate, or disseminate biometrics. You cannot forget or lose a biometric (ii). (iii) Biometrics are more secure than low-entropy passwords.

As cloud computing becomes more common in sensitive applications like Telecare Medical Information Systems (TMIS), end-user privacy is at risk from identity disclosure and tracking. They are vulnerable to attacks because they do not encrypt their connections. Authentication procedures keep people who shouldn't have access to data and systems from getting in, even when they connect through unsafe routes.

The way that people authenticate their Internet of Things (IoT) applications that are hosted in the cloud makes them targets for network attacks. Because they are so expensive to compute, the current methods don't work in situations when resources are constrained. The aim of this study is

- A simple yet effective way to implement multi-factor authentication for remote users has been created to keep cloud safe. The suggested solution can protect against many possible security breaches.
- A thorough and informal security assessment has proved that the scheme is safe from attacks and meets all security standards. A standard security study employing the prevalent random oracle model has confirmed that the proposed system is resilient against several identified security issues.

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Measured the computing effort needed for the proposed strategy and compared it to that of several other strategies. It has even more proof that the method is computationally efficient.

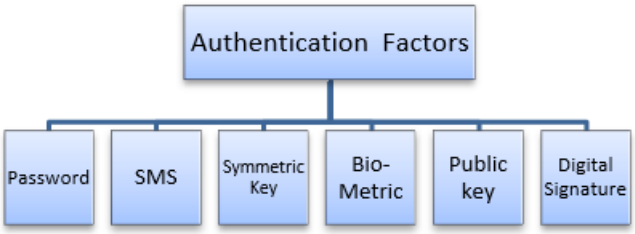

Figure 1. Authentication Factors

1.1. Password authentication

Knowledge-based authentication typically necessitates the transfer of a secret, like a password or PIN.

1.2. Symmetric-key authentication

Users can communicate to each other safely by sending encrypted copies by using the authentication server. Users regularly send random messages to servers to prove their identity. If a server gets two messages that were encrypted using the same shared secret key, it knows that the person trying to send the message is real. The server lets the user in once they have successfully authenticated.

1.3. SMS authentication

This is how the system sends the user a one-time password (OTP). There are two types of one-time passwords: challenge-response passwords, which give a challenge value in return for the user's identity, and static passwords, which are made up at random. A chronological record of all the passwords that were used to access a system makes up a list of passwords that are used to access that system. When the user enters the password then they will receive a text message indicating whether they are authenticated or not.

1.4. Biometric authentication

Biometric authentication devices take a person's fingerprints, voice, or iris and utilise them to get and store a much information about that person. There are many techniques to check a user's identity, one of which is to compare the encoding value they say they have to a known one.

1.5. Public-key authentication

Public-key cryptography requires a pair of keys, one of which must be kept secret while the other is made public. Users are given certificates to make it easier to share public keys. Two computers can connect safely, check each other's messages, and send encrypted messages by utilising a private key to convert messages and a public key to encrypt and verify signatures.

1.6. Digital signatures

To make sure the message is real, the client decrypts it with a public key and compares the result to the message's calculated digest value. The server checks the client's signature to make

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

sure that the client's data is real. You can check the integrity of downloaded files with digital signatures.

To utilise MFA, you need to know, own, or acquire at least two of the following things: knowledge or possession. The authentication factor is only shown after getting permission from the other side first. To verify transactions, you need to use MFA. To effectively verify a user's identity, multifactor authentication needs more than one authentication factor. Biometrics, passwords, and security tokens are all examples of multifactor authentication. Because almost everyone is accessing cloud data through mobile phones, the way people authenticate has changed from two-factor to three-factor [11].

- Knowledge factor: Something that is affected by someone's competence (knowledge that is only available to that person) and is therefore the best way to do most checks. To prove who they are, users normally have to give up some private information, like a password, PIN, or pattern.

- Possession factor: The stakes of ownership and management (the fact that the user has something unique) This portion, which looks like a key, has been used a lot for a long time. People who love locks and keys tend to stay out of the spotlight. A set of portable authentication tokens, about the size of a smartphone, with an LCD or e-ink screen that shows the new passcode. Token owners don't need a network because they can merely type the new code into an authentication page.

Related Work

Li et al. [12] created a mutual authentication system that used a hash function, a smart card, and a biometric to make a secure session key over an unsecured channel. This protocol was created to help set up a safe session key. Still want to point out that the hash function is used on the raw biometric data in both protocols. Biometric inputs are not appropriate as the exclusive foundation for registration and authentication due to their intrinsic subjectivity. Biometric cryptosystems are the only real option; hence, there is a need of solutions based on them instead.
Das et al. [13] came up with a way to authenticate users that uses a mix of random numbers, passwords, and biometrics. This strategy keeps the user anonymous without putting too much strain on the computer during authentication. It identified that this protocol defeats user privacy by giving away their identify via a channel that is not encrypted. Li et al. [14] showed that a protocol is open to forgeries and DoS attacks.

Lee et al. [16] recently told us that the Martnez-Peláez et al. [15] system doesn't protect users' privacy and can be abused (via replay and user impersonation). Safkhani et al. [18] showed that the Kumari et al. [17] protocol may be used to link users, guess passwords, impersonate users, and launch privileged insider attacks. With this protocol, TMIS clients can change their biometric data or turn off their smart cards from a distance. Smart cards are easy to lose, and users can interact with each other. However, a bad user can deceive the system. Khan et al. [19] developed a more robust solution to address the vulnerabilities identified in Chen et al., which include susceptibility to password guessing and impersonation of servers

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and users. Jiang et al. [20] identify the common cybercrime methods of user impersonation and password guessing.

Mir et al. [21] suggested a biometric multi-factor cloud authentication (bMACA) protocol that might be used in telemedicine systems. The proposed technique is problematic since it necessitates directly hashing raw biometric inputs, which is unfeasible. It is very important to think about problems like the fact that directly hashing biometric data is not safe, that users are not anonymous, and that impersonation and DoS attacks can happen. There is a need for a comparative examination of this work to strengthen its contributions to the improvement of safe authentication procedures.

Proposed Method

The system will utilise an authentication approach to make sure that a user before letting them in. A code, like a password, is used to check the validity of a document or signature and identify the user. Managing who can access files, programs, and data on a system.

A step-by-step technique for a lightweight authentication system that uses ECC for multi-factor authentication in a multi-cloud system.

1. Generate a public-private key pair for each user using ECC (Elliptic Curve Cryptography).
2. Store the public key of each user in a directory, which is accessible to all.
3. When a user attempts to access a cloud, the cloud initiates multi-factor authentication using combinations of the following models: password, SMS, symmetric, biometric, public key, or digital signature authentication.
4. For password authentication, the user enters their password, and the cloud verifies with stored hash of the password.
5. For SMS authentication, the user receives a one-time code on their registered phone number, enters it, and the cloud verifies it.
6. For symmetric authentication, the user generates a secret key and encrypts a random number using the key. The user sends the encrypted random number and their public key to the cloud. The cloud decrypts the random number using the user's public key and verifies it against the original random number.
7. For biometric authentication, the user provides their biometric data (e.g., fingerprint, face recognition), and the cloud verifies it against the stored data.
8. For public key authentication, the user signs a random number using their private key and sends the signed number and their public key to the cloud. The cloud verifies the signature using the user's public key.
9. For digital signature authentication, the user generates a hash of the request and signs it using their private key. The cloud verifies the signature using the user's public key.
10. If authentication is successful the cloud generates a new random number and encrypts it with the user's public key.
11. The user decrypts the random number using their private key.
12. The user generates a hash of the random number and signs it using their private key.
13. The user sends the signed hash to the cloud.

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

14. The cloud verifies the signature using the user's public key.
15. If the signature is valid, the user is authenticated.

This algorithm makes sure that only the person who has the right private key can decrypt the random number and make the hash that is needed. It also makes sure that the cloud only accepts requests from users who have been verified, which is a simple way to add multi-factor authentication in a multi-cloud system using ECC and other authentication factors.

This implementation of multi-factor authentication (MFA) systems for online banking and e-commerce uses one-time passwords (OTPs). These systems make a pseudo-random number at regular intervals, but that number is no longer useful once a specific amount of time has passed. These kinds of systems also use the more common password method, but only for a short time. In the business world, they help to solve the authentication problem on a larger scale than they do for average people. The MFA is an authentication method made up of different parts that work together to secure, the sensitive information and personal privacy.

A user profile database, is a system that keeps user information safe. The authentication method checks a user's identification before letting them into the system. An authentication server (AS) processes and checks login requests made by users in the cloud. Password is used to check that a document or signature is real and that the person is whom they say they are. Who can see and use things on a computer, like files, applications, and data.

Protecting user identities and passwords are giving access to a personal identification number for knowledge-based authentication to work, you usually have to give up a secret, like a password or PIN. You will also need a password or PIN to finish these steps.

Protection with short message service: This is how a system sends a user a one-time password (OTP). There are two kinds of one-time passwords: challenge-response passwords, which give the user identify in exchange for a challenge value, and static passwords, which are made at random. A List of passwords used to authenticate to access are arranged in a chronological order is known as password. The user is now authenticated when they type in the password they got by text message. This is used for authentication in the financial applications.

Using a Symmetric Key for Authentication: Users can safely talk to each other by sending encrypted copies of a shared secret that an authentication server makes. Users often utilise messages that are made up at random to log in to servers. When a server gets two messages that were encrypted using the same shared secret key, it knows that the person trying to send the message is real. The server lets the user in when they properly authenticate. For public-key cryptography to work, a public-key cryptosystem makes digital signatures. This requires a pair of keys, one of which must stay secret while the other is shared with the public. Certificates are given to users to make it easier for them to share their public keys. Two computers may connect safely, check each other's messages, and send encrypted messages by utilising a private key to alter messages and a public key to encrypt them and check their signatures.

Using biometric data for authentication Biometric authentication devices read a person's

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

fingerprints, voice, or iris to get and store much information about them. There are many techniques to check a user's identification, and one of them is to compare the encoding value the user claims to a recognised one.

Completion of the authentication process by providing evidence that anybody can understand, no matter their background. This increases the depth and frequency of host-to-host connections without putting any sensitive information at risk. The client makes problems that are hard to solve at random and uses the bit commitment approach to accomplish them. Then, it sends the results to the server. The server has asked the client to show proof of the problem's source and suggest a fix in return. To accomplish the authentication procedure, you need to make ten seamless handoffs. The hash function output is the basis for the solutions; hence it is a one-way function.
Digital signatures that work over the Internet (sometimes called e-signatures) This site shows a shorter and clearer version of an official record. First, the client uses the server's public key to decrypt the message. Then, it compares the decrypted message to the measured digest value to see if the message can be trusted. The server needs to check the digital signature that the client gave before it can confirm the information that the client says it possesses. The only way to be sure that the data you download is safe is to employ a digital signature.

Multi-factor authentication, or MFA, needs at least two of the following things to work: MFA needs more than one sort of authorisation, including a password, a security token, and biometric data, to work. This is different from a single-factor authentication system, which only needs one type of authorisation. The rising use of mobile devices has led to a switch from two-factor authentication to three-factor authentication [22].

People who want to use MACA for the first time in a certain place must go through the enrolment process. The enrolling program is in charge of collecting the user's profile information and fingerprint biometrics, which are shown by the letter P. The next step is to use the public key PK and P to encrypt and hash these. This is called Fully Homomorphic Encryption (FHE). The outcome is that the AS acquires the user's cryptographic profile, denoted by the P. It also gets any passwords and user IDs that were given, which are shown by psw and uid, respectively.

The Authentication Server (AS) can add user profile information to the profile database when it connects to the user profile database (UPDB). The letter P stands for user information and is what the AS adds to the profile database. P is the new user profile that has been saved as encrypted text, and psw is the password that the user typed in when they tried to log in. P stands for the new user profile, while psw stands for the password. The P means that a new user profile has been made. The AS is in charge of figuring out what makes P unique and sending back the authentication result that goes with that. The Auth Result, often known as the authentication result, is a Boolean value that tells you if the authentication worked. The acronym Auth Result [23] stands for this value.

Using fully homomorphic encryption helps keep the user profiles of each user private. Utilise a modified version of the Simple Homomorphic Encryption software package in this case. This program is free for everyone to use. The server can help with user profiles while also keeping

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

them safe from prying eyes by using methods like hashing and totally homomorphic encryption. This is because the server happens due to this. Once the cloud-based server has finished processing the encrypted text values (ψ1,ψk), the user delivers the produced action along with the encrypted text value. This creates ψ. More specifically, the two basic math operations. In particular, the subtraction and division gates (1) and (2).

$$FHE\_Decrypt(\psi 1, sk)=a-b \quad (1)$$

$$FHE\_Decrypt(\psi 2, sk)=a/b \quad (2)$$

To acquire new clients for the service, the following strategies are put into practice:

- The owner of the data gets a request to register, together with the user Terminal ID, the time stamp, the ID, and the Biometric. The owner of the data then gets this information and permission to access the data file.
- Cloud services use a multi-factor and multi-step authentication method to make sure that the person using the service is an authenticated user. The cloud centre also keeps track of and records all the contacts it has with the owner of the data.
- The owner uses their private key to scramble or encrypt the data, and the cloud checks it with a public key.
- Adding a new client to a cloud service is safe as long as the owner's private key is used to authenticate the owner and encrypt the owner's data. This is because both operations use the owner's private key.

3.1. ECC

When both a and b are primes in F_p and the value of $(4a^3+27b^2) \bmod p \neq 0$ is greater than zero, the following equation can be used to determine the value of $E_p(a,b)$: $y^2 = (x^3+ax+b) \bmod p$ multiplied by F_p.

The following is a computational impossibility by ECC:

On an elliptic curve, the Discrete Logarithm Problem, often known as the Elliptic Curve Discrete Logarithm Problem (ECDLP). Calculating Q = xP is quite easy for given $x \in Fp$ and $P \in Ep$. However, given $P \in Ep$ and $Q \in Ep$, it is computationally not easy to compute the scalar x such that Q = xP [24].

The Diffie-Hellman prime exchange problem that can be solved computationally using elliptic curves (ECCDHP): The computation of $x, y \in Fp$ for a collection of points P, xP, and yP in the space $\in E_p(a, b)$ when both x and y are treated as random is a computationally costly process where both x and y are treated as independent random variables [25].

3.2. Hash function

A hash function, which is represented by $h:\{0,1\}^* \rightarrow \{0,1\}$, takes as input a binary string of any length, which is represented by $k \in \{0,1\}^*$, and produces an output string of a fixed length,

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

which is represented by l.

The following is a list of some of the characteristics that set them apart from others:

The computational problem of finding an input k1 that, when combined with another hash value I, yields a hash value I that is identical to h presents itself as a difficulty (k1).

The computational problem of finding a pair (k1, k2) in which h(k1)=h(k2) and k1≠k2 is difficult to solve because it requires finding a pair in which k1 is smaller than k2.

Results and Discussions

In this section, by comparing the suggested model from Table 1 with the best approaches are discussed in Section 2. These are TMIS and bMACA. Five servers are used to keep the cloud data safe that comes from different devices. Cloudsim is utilised to run the simulation, and a 256-bit key is used for both public and private key. The suggested approach is calculated and compared based on how long it takes to register a user, log in, authenticate, and upload the data to the cloud. ECC-LWM works well and doesn't cost much. Building a safer architecture for the right cloud by using ECC.

S. No	Action	TMIS	bMACA	ECC-LWM
1	Registration	3.25	2.27	0.9
2	Login	1.62	1.12	1.03
3	Authentication	1.61	1.19	1.05
4	Computation	2.06	1.78	1.6

Table 1. Comparative Results of TMIS, bMACA and ECC-LWM in milliseconds.

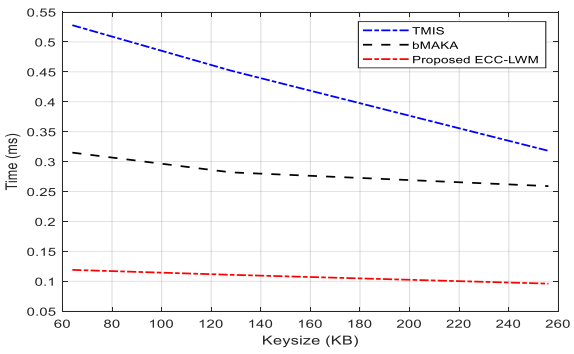

Figure 2. Time required for registration (ms)

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

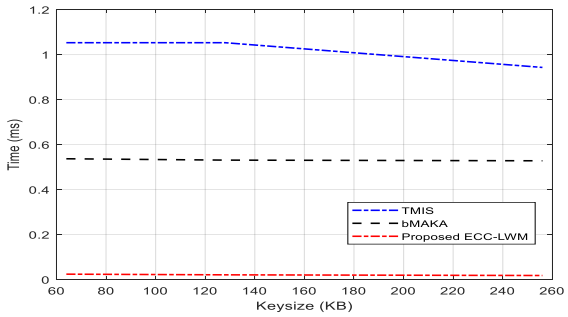

Figure 3. Time required for login (ms)

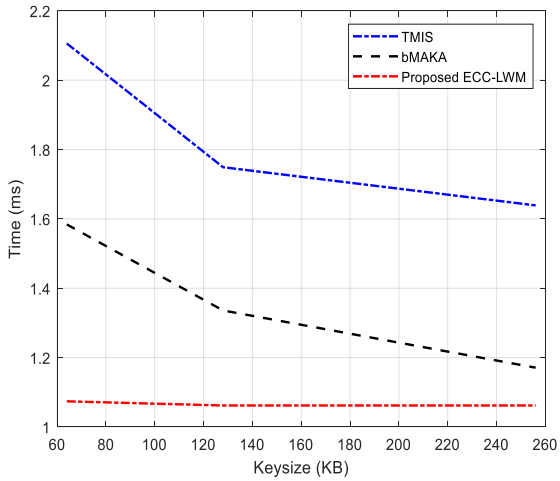

Figure 4. Time required for authentication (ms)

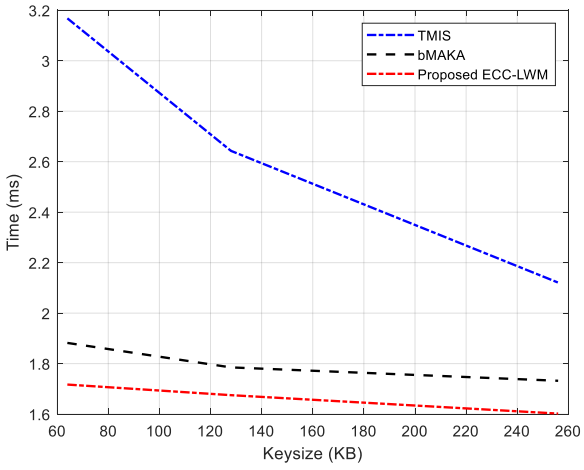

Figure 5. Time required for computational time (ms)

Figure 2-5 shows that the proposed solution reduce the time for a user to register, log in, authenticate, and upload data to the cloud. The results show that the size of the key is an important aspect in making the key smaller while yet offering a good level of security.

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Method	Replay Attack	User Impersonation	Password Guessing	DoS Attack	Biometric Forgery
TMIS	Vulnerable	Vulnerable	Vulnerable	Resistant	Vulnerable
bMACA	Partially Resistant	Partially Resistant	Vulnerable	Partially Resistant	Vulnerable
ECC-LWM	Resistant	Resistant	Resistant	Resistant	Resistant

Table 2. Resistance to various attacks

Table 2 illustrates how safe each approach is against common assaults. ECC-LWM is the best at withstanding all five types of attacks. The proposed solution provides superior security against numerous threats compared to alternative methods.

1. Conclusion

This paper presents a secure multi-factor user authentication method hosted on the cloud. Smart homes, smart cities, and smart transport systems are some of these applications are using the MFA can do. The method works well and takes less time for authentication. A random model employing ECC was utilised to verify the resilience of the method by illustrating that sensitive information cannot be retrieved from messages transmitted and received during the login and authentication procedures. The results show that the proposed method takes an average of 2.45 ms less time to compute than other methods. It also has better resistance, security features, and computing costs than similar methods, which shows that the proposed method is better than the related methods. The suggested approach has less chance to attacks, fewer security measures, and a lower cost of computing.

References

[1] Kumar, G. S., Kandavel, N., & Madhavan, K. (2020, March). To discovery the cloud services authentication an expert-based system using multi-factor authentication. In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS) (pp. 1014-1016). IEEE

[2] Loffi, L., Westphall, C. M., Grüdtner, L. D., & Westphall, C. B. (2021). Mutual authentication with multi-factor in IoT-Fog-Cloud environment. Journal of Network and Computer Applications, 176, 102932.

[3] DeviPriya, K., & Lingamgunta, S. (2020). Multi-factor two-way hash based authentication in cloud computing. International Journal of Cloud Applications and Computing (IJCAC), 10(2), 56-76.

[4] Dhillon, P. K., & Kalra, S. (2019). A secure multi-factor ECC based authentication scheme for Cloud-IoT based healthcare services. Journal of Ambient Intelligence and Smart Environments, 11(2), 149-164.

Received: August 03, 2025

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

[5] Gong, Q. (2022). Research and Practice of Cloud Application Security Based on Multi Factor Authentication Technology. Forest Chemicals Review, 1578-1584.

[6] Xu, M., Wang, D., Wang, Q., & Jia, Q. (2021). Understanding security failures of anonymous authentication schemes for cloud environments. Journal of Systems Architecture, 118, 102206.

[7] Al Nafea, R., & Almaiah, M. A. (2021, July). Cyber security threats in cloud: Literature review. In 2021 International Conference on Information Technology (ICIT) (pp. 779-786). IEEE.

[8] Raja, R. A., Karthikeyan, T., & Kousik, N. V. (2020). Improved privacy preservation framework for cloud-based internet of things. In Internet of Things (pp. 165-174). CRC Press.

[9] Mupila, F. K., & Gupta, H. (2021). A Multi-factor Approach for Cloud Security. In Innovations in Computer Science and Engineering: Proceedings of 8th ICICSE (pp. 437-445). Springer Singapore.

[10] Panguluri, S. D., Lakshmy, K. V., & Srinivasan, C. (2022). Enabling multi-factor authentication and verification in searchable encryption. In Micro-Electronics and Telecommunication Engineering: Proceedings of 5th ICMETE 2021 (pp. 717-728). Singapore: Springer Nature Singapore.

[11] Khalid, H., Hashim, S. J., Ahmad, S. M. S., Hashim, F., & Chaudhary, M. A. (2021). SELAMAT: a new secure and lightweight multi-factor authentication scheme for cross-platform industrial IoT systems. Sensors, 21(4), 1428.

[12] Li, C. T., & Hwang, M. S. (2010). An efficient biometrics-based remote user authentication scheme using smart cards. Journal of Network and computer applications, 33(1), 1-5.

[13] Das, A. K. (2011). Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards. IET Information Security, 5(3), 145-151.

[14] Li, X., Niu, J., Khan, M. K., Liao, J., & Zhao, X. (2016). Robust three-factor remote user authentication scheme with key agreement for multimedia systems. Security and Communication Networks, 9(13), 1916-1927.

[15] Martínez-Peláez, R., Toral-Cruz, H., Parra-Michel, J. R., García, V., Mena, L. J., Félix, V. G., & Ochoa-Brust, A. (2019). An enhanced lightweight IoT-based authentication scheme in cloud computing circumstances. Sensors, 19(9), 2098.

[16] Lee, H., Kang, D., Lee, Y., & Won, D. (2021). Secure three-factor anonymous user authentication scheme for cloud computing environment. Wireless Communications and Mobile Computing, 2021, 1-20.

[17] Kumari, A., Jangirala, S., Abbasi, M. Y., Kumar, V., & Alam, M. (2020). ESEAP: ECC based secure and efficient mutual authentication protocol using smart card. Journal of Information Security and Applications, 51, 102443.

Received: August 03, 2025

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

[18] Safkhani, M., Bagheri, N., Kumari, S., Tavakoli, H., Kumar, S., & Chen, J. (2020). RESEAP: an ECC-based authentication and key agreement scheme for IoT applications. IEEE Access, 8, 200851-200862.

[19] Khan, M. K., Kumari, S., & Gupta, M. K. (2014). More efficient key-hash based fingerprint remote authentication scheme using mobile device. Computing, 96, 793-816.

[20] Jiang, Q., Khan, M. K., Lu, X., Ma, J., & He, D. (2016). A privacy preserving three-factor authentication protocol for e-Health clouds. The Journal of Supercomputing, 72, 3826-3849.

[21] Mir, O., & Nikooghadam, M. (2015). A secure biometrics based authentication with key agreement scheme in telemedicine networks for e-health services. Wireless Personal Communications, 83, 2439-2461.

[22] Umamahesh.G., Rajkumar.G.V.S. (2023). Survey on Various Security Issues Associated with Cloud Authentication Techniques. In: Intelligent Systems and Sustainable Computing. ICISSC 2022. Smart Innovation, Systems and Technologies, vol 363.Springer,Singapore.

[23] Arasan, Anakath & Rajakumar, S. & Ambika, S.. (2019). Privacy preserving multi factor authentication using trust management. Cluster Computing. 22. 10.1007/s10586-017-1181-0.

[24] W. Liu, A. S. Uluagac and R. Beyah, "MACA: A privacy-preserving multi-factor cloud authentication system utilizing big data," 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 2014, pp. 518-523.

[25] Shukla, Shivangi & Patel, Sankita. (2023). A design of provably secure multi-factor ECC-based authentication protocol in multi-server cloud architecture. Cluster Computing. 27. 1-22. 10.1007/s10586-023-04034-6.

Received: August 03, 2025