Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 1702 - 1713
Received 20 January 2021; Accepted 08 February 2021.

# A Secure Two-Way Verification based Authentication Scheme with user Anonymity for Cloud Networks

*** [1]S.Mercy, [2]R.Nagaraja , [3] M.Jaiganesh**

[1,2]Department of Information Science and Engineering,

Bangalore Institute of Technology, Bangalore, Karnataka, India.

[3]Department of Information Science and Engineering, Faculty of Engineering and Technology,

Jain University, Bangalore, Karnataka, India.

[1]mercy.isaac.abraham@gmail.com, [2]prof.rnagaraja@yahoo.com, [3]jaidevlingam@gmail.com.

## Abstract

The cloud computing along with massive storage and privacy based services are upcoming technique.The information and communication technology connected with various handhold devices through Internet for performing thedata sharing between public networks with large size of users. The internet enabled devices are becoming more sophisticated applications for users in cloud computing environment. An important progression in today's cloud computing technology is the facility to connect both private and public networks for maintaining large resource or for handling large size of information. Integration of remote devices and cloud environmentbrings inclusiveusage for real-time application in many commercial products. The security alarms such as authentication and information confidentiality of these clouds computing environment plays an imperative role in successful integration of authentication and access controls. In this paper, we proposed a two-way authentication protocol using Discrete Logarithm. The proposed scheme satisfies all basic security requirements and provides mutual authentication. In this scheme, every new session a new session key will be produced for further communication. The detailed analysis of security for the proposed scheme demonstrates that it is withstand against various attacks.

## 1. Introduction

In the earlier stage of 90's, storage systems are maintained by the single server and controlled by various authentication and confidentiality schemes. Lot of research publications and research activities are proposed by the researcher. Due to the large amount of storage purpose, later 2000 cloud computing comes to the commercial purpose usage. Many issues are identified by the developers and research peoples in cloud storage and service. Practical difficulties for providing better security in cloud computing are solved by applying various cryptographic techniques. The security needs in cloud computing has been classified into two main areas of confidentiality and authentication. Most of the cloud computing applications are designed with the combination of authentication and access control for user validation. As a service provider, the cloud computing environment has to provide efficient communication between cloud users and could servers.

The fast growing of IT technology, cloud computing environment has become one of the important research areas in recent years. The cloud computing services are quickly integrated with our daily lives due to its high service efficiency, high scalability and less expensive [45]. The traditional model of service gets changed fundamentally for providing consumer access rights and services to resources: as a service granter of cloud computing. This new technology efficientlyrallies the use of resources by maintain the centralized demands. The cloud customers are gaining the accessibility of using resources and decrease the using charge through on demand.

Due to this reason, big companies are build and maintain a individual cloud environment and provide services. For example, Google App Engine, Amazon Web services,

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 1702 - 1713
Received 20 January 2021; Accepted 08 February 2021.

and IBM Smart Cloud [45] are maintaining and providing cloud service for all the customers with minimum cost. In addition to that, both the individuals and small level companies are enjoying the benefits of cloud services. In general, there are three types of cloud services are available the market: providing Infrastructure as a Service (IaaS), providing Platform for developing various applications as a Service (PaaS), providing various Software applications for the users as a Service (SaaS) [45].

Recently, most of the business solutions are transformed and changed to cloud application environment. The security issues become one of the prominent areas in cloud environment, due to the fast growing of cloud services. The following questions are most common in cloud service, how to protect user data from unauthorized access by the illegal users and how to provide user privacy. The preserving user privacy has become a challenging problem and hot area for the researchers.

These issues are solvable by applying user authentication verification schemes. The user authentication schemes are developed based on basic user verification method like, two-factor, three-factors. These schemes first verify the user identity and secret code (password, Pin number, Passcode, OTP). If the user verification successfully completed then the cloud server allow the user for accessing the cloud data and services.

In this scenario, user will be verified and malicious user request will be restricted. The cloud servers are validated by applying mutual authentication schemes. A secure authentication schemes must satisfy the above mentioned points. Once the authentication for user and cloud server is over then a session key will be established for further session secure communications.

The password-based authentication schemes are suitable for cloud environment by combine with cryptographic algorithms. In this authentication scheme, user has to register with the cloud server by including user identity and password.

## 2. Related Work

In 2011, Hao et al. [30] proposed the new authentication scheme with two-factor based on the combination of password and smart cards for the environments of cloud computing. Lot of research articles has been published with enhanced versions [35-42], each scheme different in terms of security [31], user privacy [32], usage [33], and competence [34].

A remote user authentication protocol with biometrics identity is an authentication scheme in which a remote trusted server confirms the legality of a user over a public network using his biometric identity. Last few years, several research papers have been published by the scholars in the field of biometrics-based remote user authentication protocol using smart cards [11–24]. A remote user authenticationschemes with user biometric proposed for different kinds of real-time environment such as protected multi-server environments [25–29] and Telecare Medicine Information System (TIMS) [7][30–33]. An effective three-factor authentication protocol for remote user verification are proposed in [34, 35] using Discrete Logarithm Problem (DLP) and Elliptic Curve Cryptosystem (ECC).

In 2010, Li and Hwang [2] introduced an efficient bio-metric based authentication scheme for remote users using smart cards. Later, Li et al. [3] and Das [4] shows that Li and Hwang's [2] scheme suffers with few security flaws and they have proposed two new improved authentication protocol based on the classical biometrics technology. In the proposed schemes, the user biometric identity is matched with the original biometric identity stored in the server system storage with basic security developments to overwhelm the noticed security defects.

In 2012, An [5] shows that Das's [4] scheme has some security weakness, like password guessing, user impersonation, and insider attacks. To overcome the security weakness in the Das's [4] scheme An [5] proposed an upgraded scheme. In 2013, Khan and

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 1702 - 1713
Received 20 January 2021; Accepted 08 February 2021.

Kumari [6] pointed out that there some gaps are present in the An's [5] protocol and they have introduced an upgraded biometric-based remote user authentication scheme to overcome the pitfalls by incorporating the user anonymity property. Recently, Sarvabhatla et al. [8] and Wen et al. [9] pointed out that Khan and Kumari's [6] scheme is subject to against guessing of password attacks and user masquerade attacks. They have proposed two new authentication schemes to overwhelmed the security faintness of Khan and Kumari's [6] scheme. The above illustrated protocols make use of user's biometrics identity to defend the user's password and improve the user's secrecy and privacy.

In 2013, Yang et al. [20] dedicated to introduce a secure authentication protocol for the environment of cloud computing, this scheme is weak to dictionary attack. Then Yang et al. [21] introduced a new protocol; inappropriately, Chen et al. [22] revealed this scheme is subject to insider attack and impersonation attack. Chen et al [22][56] proposed a new version to protocol to overcome the weakness.Chen et al [22] scheme is broken by Wang et al. [33]. Wang et al. [33] showed that Chen et al.'s scheme [12] is vulnerable to offline dictionary attack and impersonation attack. Recently, Amin et al. [39][57]shows that the security flaws in the schemes of Xue et al. [24] and Chuang et al. [25]. These two schemes are fail to provide user anonymity and forward secrecy while being not able to resist against offline password guessing attack and so on. Therefore, they designed a new scheme that claims to overcome the security flaws of the two schemes and be secure to various attacks.

Most of the biometrics identity based or three-factor authentication schemes [3, 6, 7, 9, 10] are fails to withstand security issues, because of the using cryptographic hash function directly on the biometric identity. The hash digested values are computed directly from the biometric identities, but no two biometrics readings will have the same feature and they are rarely identical.

In 2015, Das and Goswami [10] proposed a robust remote authentication scheme based on biometric identity using smart cards. The biometric identity is protected by using fuzzy extractor techniques and Bio-Hashing function. Das and Goswami [10] scheme requires so expensive communication and computation and this schemeneeds the user has to remember a complex password. Zhao et al. [11][55] proposed a new method by applying a fuzzy negotiation structure by using the concept of fuzzy extractor technology to secure a Body Sensor Network (BSN). In the pre-stage process of the structure, each biosensor node has been preloaded with secret keys for the purpose of security and verify the commitment.

In 2016, Roy et al. [12][53][54] presented a remote user authentication by applying biometrics for a TMIS applications using Bio-Hashing function. Qi and Tang [13] proposed a new session initiation protocol based on biometrics authentication using a fuzzy extractor technique. Roy et al. and Qi and Tang schemes needs high computational and communication costs. In [43], Henniger and Waldmann proposed a method with biometric identity based authentication protocol using smart cards.

In recent years, extensive efforts have been taken for a secure and practical authentication scheme in cloud computing environment, some of the recent schemes are [26–29]. Most of the researchers are claims that, these scheme are having security flaws more or less. Design and developing a secure authentication scheme is still a challengefor cloud computing environment. Recent years, many peoples are using cloud computing fir real-time application like, hospital, online-shopping, etc., the potential security pressures will lead to greater damage. This unacceptable situation motivates us to explore the inherent reasons of the failure in those schemes, find the basic method to fix the security flaws, and design a robust and efficient user authentication protocol for cloud computing environment.

In this paper, we have proposed a two-way authentication scheme using Discrete Logarithm. The proposed scheme satisfies all basic security requirements and provides mutual authentication. In this scheme, every new session a new session key will be generated

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 1702 - 1713
Received 20 January 2021; Accepted 08 February 2021.

for further communication. The security analysis of the proposed scheme demonstrates that it is secure against various attacks.

## 3. Proposed Two-way Authentication scheme

### 3.1. Preliminaries

In this section, we providing some fundamental cryptographic properties, like Collision resistant property, Discreate Logarithm Problem and Bio-Metric Fuzzy Extractor.

**1. Hash function with Collision resistant**

In general, the definition for the collision resistant hash function as follows [44]: Definition : A cryptographic hash function is defined as follows, $h(\{0,1\}^*) : \rightarrow \{0,1\}^k$, this function known to be a collision resistant hash function if and only if, the following properties are satisfied:

a. Compression: The function $h(.)$produces the output of $h(x)$ with fixed length of $k - bits$ for the input of $x$ of random finite bit length.
b. Pre-image resistance: For all the specified outputs of $h(.)$, it is computationally infeasible for finding any input $x'$ such that it produce $h(x') = y$.
c. Collision resistant: It is computationally infeasible for finding any two different inputs $x$ and $x'$produce the same hash value, i.e. $h(x) = h(x')$.

**2. Discrete Logarithm Problem**

Definition : The Discrete Logarithm Problem over a group $Z_p^*$, can be illustrated as follows: Let us assume that $Z_p^*$ is a finite cyclic group with respect to the order of $p$, here $p$ is sufficiently large prime number. Here $g$ is a generator of finite cyclic group $Z_p^*$, and $y$ is a positive integer belongs to the group of $Z_p^*$. Then the modular exponentiation for the $y$ is denotes as follows,

$$x = g^y (mod\ p), x \in Z_p^*$$

Let us assume that, the known value of $(x, p, g)$ are public variable. From the known values finding of $y$ is computationally infeasible. This will takes polynomial time for solving the problem.

### 3.2. Proposed Scheme

The proposed authentication scheme has three phases, Registration Phase, Login Phase, Authentication and verification Phase. The following section explains proposed phases in detail. The registration phase will be executed only once during the user registration. The user may access the cloud services by executing login phase and each new login request the user will get new session key. This key can be used for further secure session communication.

**a. Registration Phase**

In the registration phase, theuser $U_i$, selects his identity $ID_i$ and password $PW_i$. The user $U_i$has to perform the following steps,

1. Compute $CID_i = ID_i || T_R$ and $CPW_i = PW_i || T_R$
2. The user $U_i$ request the Cloud Server $CS$ bysending a registration request along with the following parameters
$$\{CID_i, CPW_i, T_R\}$$
3. The Cloud Server$CS$receives the registration request and stores$CID_i, CPW_i$ and $T_R$in a database maintained by the Cloud Server
4. The Cloud Server send a accepted and conformation message to the user $U_i$ along with the Public Key of Cloud Server$(Key_P)$.
5. The user $U_i$maintain the Public Key of Cloud Server $(Key_P)$ for further communication with the Cloud Server

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 1702 - 1713
Received 20 January 2021; Accepted 08 February 2021.

**b. Login Phase**

The legal users are allows to enter into the Cloud Server through login phase only. During the client login phase, the user $U_i$ has to enter his/her Identity$CID_i$ and Password $CPW_i$through service request login page. The client login page will perform the following steps,

1. The client login paper computes $CID_i^{new} = ID_i \oplus T_C$ and $CPW_i^{new} = PW_i \oplus T_C$
2. The client computes $C_1 = h(CID_i^{new} || CPW_i^{new})$ and encrypt the $C_1$ by using public key of Cloud Server $Key_P$ as follows $E_1 = Enc_{Key_P}(C_1)$
3. Select a random nonce $r$ and compute the following value, $C_2 = h(C_1||T_C||r)$
4. Encrypt the $C_2$ by using public key of Cloud Server as follows, $E_2 = Enc_{Key_P}(C_2)$
5. The login request message has been generated along with the following parameters,

$$Login\ Request\ Message = \{E_1, E_2, T_C\}$$

**c. Verification and Mutual Authentication Phase**

In this phase, the Cloud Server $(CS)$receives the login request message and verifies it as follows

1. The Cloud Server CS receives the login request message $\{E_1, E_2, T_C\}$ at $T_C^*$and verify the authentication as follows,
    a. If $(T_c - T_c^* \leq \Delta T)$ then ACCEPT the Login request and proceed further
    b. Else REJECT the login request message
    c. The Cloud Server decrypts the received message by using the private key $Key_{Pr}$as follows,
    $$D_1 = Dec_{Key_{Pr}}(E_1) \text{and} D_2 = Dec_{Key_{Pr}}(E_2)$$
    d. If $(D_1 == h(CID_i^{new} || CPW_i^{new}))$then ACCEPT the Login request and go to Step 2
    e. Else REJECT the request
2. The Cloud Serverselects a random number $r_2$ and compute session key as follows
$$SK_{New} = g^{h(D_2 \oplus r_2 \oplus T_S)}(mod\ P)$$
3. The Cloud Server computes$C_3 = h(D_2||r_2||T_S)$ and $E_3 = SEnc_{SK_{New}}(C_3)$
4. The Cloud Server generate a mutual authentication message $MA_{New} = \{E_3, r_2, T_S\}$
5. The Client user$U_i$ receives the message $MA_{New} = \{E_3, r_2, T_S\}$at $T_S^*$from the Cloud Server CS and perform the following checking process,
    a. If $(T_s - T_s^* \leq \Delta T)$ then ACCEPT the Login request and proceed further
    b. Else REJECT the mutual authentication message
    c. Compute session key as follows, $SK_{New} = g^{h(E_2 \oplus r_2 \oplus T_S)}(mod\ P)$, here $r_2$ and $T_S$values are taken from $MA_{New}$.
    d. The user $U_i$ decrypts $E_3$as follows, $D_3 = SEnc_{SK_{New}}(E_3)$ and compute $D_4 = h(C_2||r_2||T_S)$
    e. The user $U_i$compare $C_3$ and $D_4$ as follows,
    $$if(C_3 == D_4)\ then\ ACCEPT$$
    f. Else REJECT the Mutual Authentication message

The common session key will be agreed upon with the user $U_i$and Cloud Server CS

**4. Security Analysis**

**a. User Anonymity and maintaining Session Key**

In the proposed authentication scheme, the attackers cannot obtain any user private information like the user's identity form the known information of login request $Login\ Request\ Message = \{E_1, E_2, T_C\}$.In this login request message, both $E_1$ and $E_2$ has been encrypted by using servers public key. If an attacker captures the login request message and tries to decrypt the $E_1$ for identify the user identityMutual authentication

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 1702 - 1713
Received 20 January 2021; Accepted 08 February 2021.

The user $U_i$has been verified by the server and the server has been verified by the user $U_i$, this process known as mutual authentication. The mutual authentication verification has been included in the proposed authentication scheme during the Authentication and verification message. During this phase Session for the future session communication has been created. The session key has been created by using the following method $SK_{New} = g^{h(D_2 \oplus r_2 \oplus T_S)}(mod\ P)$ and we have used discrete logarithm concepts.

Assume, an attacker tries to generate original session key from the collected information from the login request and mutual authentication messages. Due to the discrete logarithm problem, it is highly impossible for the attackers for calculating the exact session key.

**b. Resistance against replay attacks**

A replay attack is a kind of message fabrication for making an illegal message conversation between two legal parties. In the proposed, the attacker capture the previously generated login request message $Login\ Request\ Message = \{E_1, E_2, T_C\}$ and send the message with current time stamp to the server. The server decrypt the $E_1$ and $E_2$ by using his private key and check with the recalculated values. This will not be match, due to the new time stamp. The login request message will be a new one for every new login session. Both $E_1$ and $E_2$ are generated based on the current time stamp only. In the proposed authentication scheme replay attack is not possible

**c. Resistance against forgery attacks**

From the legal userside, he/she attempts to act as another legal user in the same cloud. The attacker has generate a forged a authenticate request message$Login\ Request\ Message = \{E_1, E_2, T_C\}$ and send to the server. However, the forged messages will not be authenticated by the server due to the message freshness along with user identity and password. The login request message has been created with $E_1 = Enc_{Key_P}(C_1)$ and $E_2 = Enc_{Key_P}(C_2)$and these values could not be created by any legal user for other legal user.

**d. Resistance against denial-of-service attacks**

During the login phase, any one of the attacker tries to implement the denial of service for any legal user by capturing the login. If an attacker generate an illegal replay message and send to the user, then the user verifies the mutual authentication and ignore the replay message from the illegal sever.

**e. Resistance to server spoofing attacks**

If an attacker attempts to impersonate like server by replaying a forged mutual authentication message for the login request message $Login\ Request\ Message = \{E_1, E_2, T_c\}$. This is not possible in the proposed authentication scheme due to the verification technique. Both user and the server verifies the time stamp and encrypted request, if any one of the verification is fails then user can easily come to know server service spoofed.

**f. Forward secrecy**

The session key has been created by the server will not be shared directly with user, instead of that a small portion of information has been shared. The user has to generated the same session key with this shared information. This will be verified by the user and server during the mutual authentication phase. If an attacker tries to capture the session communication and tries to guess the post session key, then it is not possible in the proposed authentication scheme, due to the freshness in the session key. The new session has been started with new time stamp and nonce value. So, the forward secrecy has been maintained by the proposed scheme.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 1702 - 1713
Received 20 January 2021; Accepted 08 February 2021.

## 5. Performance Analysis

In this section, we have provided the detailed study on performance analysis for the proposed authentication scheme. The performance analysis phase includes basic cryptographic operations with respect to the execution time taken. The related authentication schemes are compared with proposed authentication for login and authentication phases. We have not consider the registration phase for the performance analysis. Following related authentication schemes are consider for performance analysis,Juang et al.'s scheme [24], Sun et al.'s scheme [4], Singh et al.'s scheme [13], and Li et al.'s scheme [25].

The following table 1 provides basic cryptographic operations with respect to the execution time. The execution time has been calculated from the basic computing environment with Windows 3 64-bit PC, Intel Core i5-8250U CPU of 1.60 GHz, 4GB RAM.

The cryptographic functions/cryptography operations are developed with core JAVA cryptographic functions. The Java Cryptographic Architecture (JCA) is a cryptographic platform, which provides a set of Application Program Interface (API's) for hash functions, point multiplications, modular inverse, key generation and random number generation. These API's are allowed the developers to develop and integrate the security needs. In the proposed method, we have used basic cryptographic operations directly and the performance has been measured with respect the milliseconds.

$T_H$: Execution time taken to perform Hash Operation

$T_{RSA}$: Execution time taken to perform Encryption/Decryption using RSA

$T_{ECC}$: Execution time taken to perform Encryption/Decryption using ECC

$T_{Sym}$: Execution time taken to perform Encryption/Decryption using Symmetric Algorithm

$T_{DLP}$: Execution time taken to perform aDiscrete Logarithm Problem

| Cryptography Operations | Execution time in Milliseconds |
|---|---|
| $T_H$ | $0.54\ ms$ |
| $T_{RSA}$ | $15.75\ ms$ |
| $T_{ECC}$ | $17.55\ ms$ |
| $T_{Sym}$ | $7.55\ ms$ |
| $T_{DLP}$ | $13.55\ ms$ |

**Table 1**: Execution Time for each Cryptography Operations

The following Table 2, provides the execution time comparison for the related schemes. The Huang et al [46] scheme requires$3T_H + 1T_{Sym}$ for login phase and $1T_{ECC} + 1T_{Sym}$ for authentication phase.Juang et al.'s scheme [47] needs$3T_H + 1T_{Sym}$ for login phase and$1T_{ECC} + 2T_{Sym}$ for authentication phase.Sun et al.'s scheme [48] required $2T_{ECC} + 4T_H$ for login phase and $2T_{ECC} + 1T_{Sym}$ for authentication phase.

Singh et al.'s scheme [49] needs$2T_{ECC} + 4T_H$ and $2T_{ECC} + 1T_{Sym}$ for login and authentication phase respectively. Li et al [50] scheme required $8T_H + 4T_{Sym}$ for login phase and $1T_{ECC} + 10T_{Sym}$ for authentication phase. Lu et al [51] scheme needs $1T_{PM} + 5T_H$ and $3T_{PM} + 6T_H$ for login and authentication phases respectively. Sutrala et al [52] scheme required $7T_H + 1T_e$ for login phase and $9T_H + 1T_e$ for authentication phase. The proposed authentication scheme required $2T_H + 2T_{RSA}$ for login phase and $2T_H + 1T_{DLP} + 1T_{Sym}$ for authentication phase. The following table 3 and the figure 1 illustrate the performance analysis for the related authentication schemes with proposed authentication scheme.

| **Authentication Scheme** | **Login Phase** | **Authentication and Key Agreement Phase** | **Total Cost** |
|---|---|---|---|

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 1702 - 1713
Received 20 January 2021; Accepted 08 February 2021.

| | | | |
|---|---|---|---|
| Huang et al [46] | $3T_H + 1T_{Sym}$ | $1T_{ECC} + 1T_{Sym}$ | $3T_H + 1T_{ECC} + 2T_{Sym}$ |
| Juang et al [47] | $3T_H + 1T_{Sym}$ | $1T_{ECC} + 2T_{Sym}$ | $3T_H + 1T_{ECC} + 3T_{Sym}$ |
| Sun et al [48] | $2T_{ECC} + 4T_H$ | $2T_{ECC} + 1T_{Sym}$ | $4T_H + 4T_{ECC} + 1T_{Sym}$ |
| Singh et al [49] | $2T_{ECC} + 4T_H$ | $2T_{ECC} + 1T_{Sym}$ | $4T_{ECC} + 4T_H + 1T_{Sym}$ |
| Li et al [50] | $8T_H + 4T_{Sym}$ | $1T_{ECC} + 10T_{Sym}$ | $8T_H + 14T_{Sym} + 1T_{ECC}$ |
| Lu et al [51] | $1T_{RSA} + 5T_H$ | $3T_{RSA} + 6T_H$ | $4T_{RSA} + 11T_H$ |
| Sutrala et al [52] | $7T_H + 1T_{ECC}$ | $9T_H + 1T_{ECC}$ | $16T_H + 2T_{ECC}$ |
| Proposed Scheme | $2T_H + 2T_{RSA}$ | $2T_H + 1T_{DLP} + 1T_{Sym}$ | $4T_H + 2T_{RSA} + 1T_{DLP} + 1T_{Sym}$ |

**Table 2**: Computational cost comparison with the related schemes

| Authentication Scheme | Total Cost | Total Execution Time |
|---|---|---|
| Huang et al [46] | $3T_H + 1T_{ECC} + 2T_{Sym}$ | 34.27 $ms$ |
| Juang et al [47] | $3T_H + 1T_{ECC} + 3T_{Sym}$ | 41.82 $ms$ |
| Sun et al [48] | $4T_H + 4T_{ECC} + 1T_{Sym}$ | 79.91 $ms$ |
| Singh et al [49] | $4T_{ECC} + 4T_H + 1T_{Sym}$ | 79.91 $ms$ |
| Li et al [50] | $8T_H + 14T_{Sym} + 1T_{ECC}$ | 127.57 $ms$ |
| Lu et al [51] | $4T_{PM} + 11T_H$ | 68.94 $ms$ |
| Sutrala et al [52] | $16T_H + 2T_{ECC}$ | 43.74 $ms$ |
| Proposed Scheme | $4T_H + 2T_{RSA} + 1T_{DLP} + 1T_{Sym}$ | 54.76 $ms$ |

**Table 3**: Execution Time comparison with the related schemes

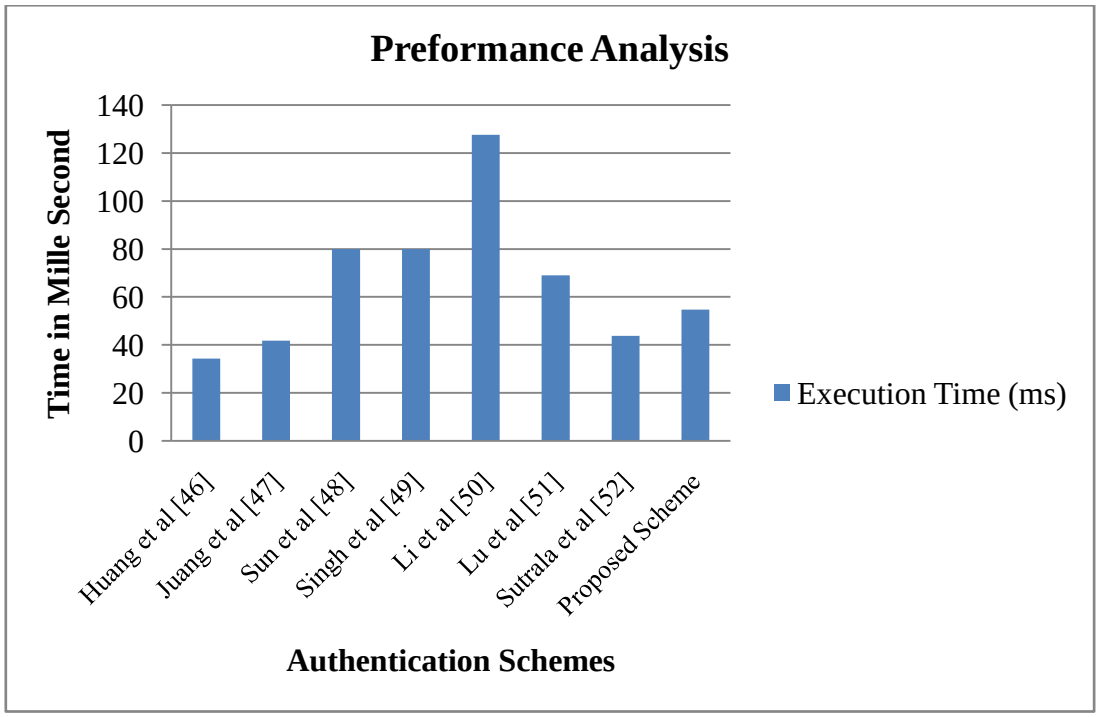


**Figure 1**: Performance Analysis for the related authentication schemes with proposed scheme

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 1702 - 1713
Received 20 January 2021; Accepted 08 February 2021.

## 6. Conclusion

In this paper, we have proposed an authentication scheme using simple password along with public key cryptographic algorithm for cloud computing environment. The proposed authentication scheme has three basic phases. The login and authentication verification phase has been executed for every new login session. The proposed authentication scheme is two-factor authentication scheme with user identity and password. The session key has been created with discrete logarithm. The proposed authentication scheme is secure with various kinds of attacks in cloud environment. We have provided a informal security analysis for the proposed authentication scheme. The proposed scheme requires minimum computational cost and communication cost. In future, the proposed scheme may be improved with different public key cryptographic algorithms.

## Reference

[1] Yeh, H., Chen, H., Hu, J., et al.: 'Robust elliptic curve cryptography-based three factor user authentication providing privacy of biometric data', IET Inf. Secur., 2013, 7, (3), pp. 247–252

[2] Li, C., Hwang, M.: 'An efficient biometrics-based remote user authentication scheme using smart cards', J. Netw. Comput. Appl., 2010, 33, (1), pp. 1–5

[3] Li, X., Niu, J., Ma, J., et al.: 'Cryptanalysis and improvement of a biometricsbased remote user authentication scheme using smart cards', J. Netw. Comput. Appl., 2011, 34, (1), pp. 73–79

[4] Das, K.: 'Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards', IET Inf. Secur., 2011, 5, (3), pp. 145–151

[5] An, Y.: 'Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards', J. Biomed. Biotechnol., 2012, 2012, pp. 1–6, doi: 10.1155/2012/519723

[6] Khan, M., Kumari, S.: 'An improved biometrics-based remote user authentication scheme with user anonymity', Biomed. Res. Int., 2013, 2013, p. 9, Article ID 491289

[7] Xi, K., Ahmad, T., Han, F., et al.: 'A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment', Secur. Commun. Netw., 2011, 4, (5), pp. 487–499

[8] Sarvabhatla, M., Giri, M., Vorugunti, C.: 'A secure biometrics-based remote user authentication scheme for secure data exchange'. Proc. IEEE Int. Conf. Embedded Systems, India, July 2014, pp. 110–115

[9] Wen, F., Willy, S., Guomin, Y.: 'Analysis and improvement on a biometricbased remote user authentication scheme using smart cards', Wirel. Pers. Commun., 2015, 80, (4), pp. 1747–1760

[10] Das, K., Goswami, A.: 'Robust anonymous biometric-based remote user authentication scheme using smart cards', J. King Saud Univ., Comput. Inf. Sci., 2015, 27, (2), pp. 193–210

[11] Zhao, H., Chen, C., Hu, J., et al.: 'Securing body sensor networks with biometric methods: a new key negotiation method and a key sampling method for linear interpolation encryption', Int. J. Distrib. Sensor Netw., 2015, 11, (8), article no. 12, doi:10.1155/2015/764919

[12] Roy, S., Chatterjee, S., Chattopadhyay, S., et al.: 'A biometrics-based robust and secure user authentication protocol for e-healthcare service'. Proc. IEEE Int. Conf. Advances in Computing, Communications and Informatics, India, 2016, pp. 638–644

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 1702 - 1713
Received 20 January 2021; Accepted 08 February 2021.

[13] Qi, X., Tang, Z.: 'Biometrics based authentication scheme for session initiation protocol', SpringerPlus, 2016, 5, (1), p. 1045
[14] Odelu, V., Das, K., Goswami, A.: 'A secure biometrics-based multi-server authentication protocol using smart cards', IEEE Trans. Inf. Forensics Secur., 2015, 10, (9), pp. 1953–1966
[15] Chaudhry, A.: 'A secure biometric based multi-server authentication scheme for social multimedia networks', Multimedia Tools Appl., 2015, 75, (20), pp. 12705–12725
[16] Lu, Y., Li, L., Yang, X., et al.: 'Robust biometrics based authentication and key agreement scheme for multi-server environments using smart cards', PloS One, 2015, 10, (5)
[17] Chaturvedi, A., Das, K., Mishra, D., et al.: 'Design of a secure smart cardbased multi-server authentication scheme', J. Inf. Secur. Appl., 2016, 30, pp. 64–80
[18] Kumari, S., Li, X., Wu, F., et al.: 'Design of a provably secure biometricsbased multi-cloud-server authentication scheme', Future Gener. Comput. Syst., 2017, 68, pp. 320–330
[19] Das, K.: 'A secure user anonymity-preserving three-factor remote user authentication scheme for the telecare medicine information systems', J. Med. Syst., 2015, 39, (3), pp. 1–20
[20] J. H. Yang, Y. F. Chang, and C. C. Huang, "A user authentication scheme on multi-server environments for cloud computing," in *Proceedings of the ICICS 2013*, pp. 1–4, 2013.
[21] J. H. Yang and P. Y. Lin, "An ID-Based User Authentication Scheme for Cloud Computing," in *Proceedings of the IIH-MSP 2014*, pp. 98–101, 2014.
[22] T.-H. Chen, H.-L. Yeh, and W.-K. Shih, "An advanced ECC dynamic ID-Based remote mutual authentication scheme for Cloud Computing," in *Proceedings of the MUE 2011*, pp. 155–159, 2011.
[23] D. Wang, Y. Mei, C. Ma, and Z. Cui, "Comments on an Advanced Dynamic ID-Based Authentication Scheme for Cloud Computing," in *Proceedings of the WISM 2012*, pp. 246–253, 2012.
[24] K.-P. Xue, P.-L. Hong, and C.-S. Ma, "A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture," *Journal of Computer and System Sciences*, vol. 80, no. 1, pp. 195–206, 2014.
[25] M.-C. Chuang and M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics," *International Journal of Network Security*, vol. 18, no. 5, pp. 997–1000, 2014.
[26] J.-L. Tsai and N.-W. Lo, "A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services," *IEEE Systems Journal*, vol. 9, no. 3, pp. 805–815, 2015.
[27] V. Odelu, A. K. Das, S. Kumari, X. Huang, and M. Wazid, "Provably secure authenticated key agreement scheme for distributed mobile cloud computing services," *Future Generation Computer Systems*, vol. 68, pp. 74–88, 2017.
[28] P. Gope and A. K. Das, "Robust Anonymous Mutual Authentication Scheme for n-Times Ubiquitous Mobile Cloud Computing Services," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1764–1772, 2017.
[29] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, "On the Design of Provably Secure Lightweight Remote User Authentication Scheme for Mobile Cloud Computing Services," *IEEE Access*, 2017.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 1702 - 1713
Received 20 January 2021; Accepted 08 February 2021.

[30] Z. Hao, S. Zhong, and N. Yu, "A time-bound ticket-based mutual authentication scheme for cloud computing," *International Journal of Computers, Communications and Control*, vol. 6, no. 2, pp. 227–235, 2011.
[31] D. Wang, Q. Gu, H. Cheng, and P. Wang, "The request for better measurement: A comparative evaluation of two-factor authentication schemes," in *Proceedings of the ACM, ASIACCS '16*, pp. 475–486, 2016.
[32] H. Xiong, J. Tao, and C. Yuan, "Enabling telecare medical information systems with strong authentication and anonymity," *IEEE Access*, vol. 5, pp. 5648–5661, 2017.
[33] D. Wang and P. Wang, "On the usability of two-factor authentication," in *Proceedings of the SecureComm*, pp. 141–150, 2014.
[34] G. Xu, J. Liu, Y. Lu, X. Zeng, Y. Zhang, and X. Li, "A novel efficient MAKA protocol with desynchronization for anonymous roaming service in Global Mobility Networks," *Journal of Network and Computer Applications*, vol. 107, pp. 83–92, 2018.
[35] J. Yu, G. Wang, Y. Mu, and W. Gao, "An efficient generic framework for three-factor authentication with provably secure instantiation," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2302–2313, 2014.
[36] D. Wang and P. Wang, "Two birds with one stone: two-factor authentication with security beyond conventional bound," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 708–722, 2018.
[37] Q. Xie, D. S. Wong, G. Wang, X. Tan, K. Chen, and L. Fang, "Provably secure dynamic ID-based anonymous two-factor authenticated key exchange protocol with extended security model," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 6, pp. 1382–1392, 2017.
[38] V. Odelu, A. K. Das, S. Kumari, X. Huang, and M. Wazid, "Provably secure authenticated key agreement scheme for distributed mobile cloud computing services," *Future Generation Computer Systems*, vol. 68, pp. 74–88, 2017.
[39] R. Amin, S. H. Islam, P. Gope, K. R. Choo, and N. Tapas, "Anonymity preserving and lightweight multi-medical server authentication protocol for telecare medical information system," *IEEE Journal of Biomedical and Health Informatics*, p. 1, 2018.
[40] Q. Jiang, Y. Qian, J. Ma, X. Ma, Q. Cheng, and F. Wei, "User centric three-factor authentication protocol for cloud-assisted wearable devices," *International Journal of Communication Systems*, vol. 32, pp. 1–20, 2019.
[41] Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He, "A privacy preserving three-factor authentication protocol for e-Health clouds," *The Journal of Supercomputing*, vol. 72, no. 10, pp. 3826–3849, 2016.
[42] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K. R. Choo, and Y. Park, "Design of secure and lightweight authentication protocol for wearable devices environment," *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 4, pp. 1310–1322, 2018.
[43] Henniger, O., Waldmann, U.: 'Supplemental biometric user authentication for digital-signature smart cards'. Proc. BIOSIG, Darmstadt, Germany, 2009, pp. 177–180
[44] S. Islam and M. Khan, ''Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems,'' J. Med. Syst., vol. 38, no. 10, p. 135, 2014, doi: 10.1007/s10916-014- 0135-9
[45] "IaaS, PaaS and SaaS – IBM Cloud service models," https://www.ibm.com/in-en/cloud/learn/iaas-paas-saas

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 1702 - 1713
Received 20 January 2021; Accepted 08 February 2021.

[46] Jheng-Jia Huang, Wen-ShenqJuang, Chun-I Fan and Horng-TwuLiaw, "Robust and Privacy Protection Authentication in Cloud Computing," International Journal of Innovative Computing, Information and Control Volume 9, Number 11, pp. 4247–4261

[47] W. S. Juang, S. T. Chen and H. T. Liaw, Robust and efficient password-authenticated key agreement using smart cards, IEEE Transactions on Industrial Electronics, vol.55, pp.2551-2556, 2008

[48] D. Z. Sun, J. P. Huai, J. Z. Sun, J. X. Li, J. W. Zhang and Z. Y. Feng, Improvements of Juang et al.'s password-authenticated key agreement scheme using smart cards, IEEE Transactions on Industrial Electronics, vol.56, pp.2284-2291, 2009.

[49] K. Singh, A. Khalique and S. Sood, A password-authenticated key agreement scheme based on ECC using smart cards, International Journal of Computer Applications, vol.2, pp.26-30, 2010.

[50] X. Li, W. Qiu, D. Zheng, K. Chen and J. Li, Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards, IEEE Transactions on Industrial Electronics, vol.57, pp.793-800, 2010.

[51] Y. Lu, L. Li, H. Peng, Y. Yang, "An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem," J. Med. Syst. 39 (3) (2015) 1–8.

[52] Anil Kumar Sutrala, Ashok Kumar Das, VangaOdelu, Mohammad Wazid, SaruKumari, "Secure anonymity-preserving password-based user authentication and session key agreement scheme for telecare medicine information systems," computer methods and programs in bio medicine 135 (2016) pp. 167–185.

[53] K.Venkatachalam, A.Devipriya, J.Maniraj, M.Sivaram, A.Ambikapathy, Iraj S Amiri, "A Novel Method of motor imagery classification using eeg signal", Journal Artificial Intelligence in Medicine Elsevier, Volume 103, March 2020, 101787

[54] Yasoda, K., Ponmagal, R.S., Bhuvaneshwari, K.S. K Venkatachalam, " Automatic detection and classification of EEG artifacts using fuzzy kernel SVM and wavelet ICA (WICA)" Soft Computing Journal (2020).

[55] P. Prabu, Ahmed Najat Ahmed, K. Venkatachalam, S. Nalini, R. Manikandan,Energy efficient data collection in sparse sensor networks using multiple Mobile Data Patrons, Computers & Electrical Engineering,Volume 87,2020.

[56] V.R. Balaji, Maheswaran S, M. Rajesh Babu, M. Kowsigan, Prabhu E., Venkatachalam K,Combining statistical models using modified spectral subtraction method for embedded system,Microprocessors and Microsystems, Volume 73,2020.

[57] Malar, A.C.J., Kowsigan, M., Krishnamoorthy, N. S. Karthick, E. Prabhu & K. Venkatachalam (2020). Multi constraints applied energy efficient routing technique based on ant colony optimization used for disaster resilient location detection in mobile ad-hoc network. Journal of Ambient Intelligence and Humanized Computing, 01767-9.