Computer Systems Science & Engineering
DOI: 10.32604/csse.2022.021845
Article

Tech Science Press

Secure Key Management Based Mobile Authentication in Cloud

S. Shanmuga Priya[1], D. Yuvaraj[2,*], T. Satyanarayana Murthy[3], Varghese S. Chooralil[4], S. Navaneetha Krishnan[5], P. Banumathy[6] and P. SundaraVadivel[7]

[1]Department of Computer Science and Engineering, M.I.E.T Engineering College, Trichy, Tamilnadu, India
[2]Department of Computer Science and Engineering, Cihan University, Duhok, Kurdistan Region, Iraq
[3]Department of Computer Science and Engineering, Bapatla Engineering College, Bapatla, Andhra Pradesh, India
[4]Department of Computer Science and Engineering, Rajagiri School of Engineering and Technology, Kakkanad, Kerala, India
[5]Department Electronics and Communication Engineering, SACS MAVMM Engineering College, Madurai, Tamilnadu, India
[6]Department of Information Technology, Karaikal Polytechnic College, Varichikudy-Karaikal, India
[7]Department of Computer Science and Engineering, SACS MAVMM Engineering College, Madurai, India
*Corresponding Author: D. Yuvaraj. Email: yuva.r.d@gmail.com

Received: 16 July 2021; Accepted: 16 November 2021

Abstract: Authentication is important to the security of user data in a mobile cloud environment. Because of the server's user credentials, it is subject to attacks. To maintain data authentication, a novel authentication mechanism is proposed. It consists of three independent phases: Registration, login, and authentication and key agreement. The user registers with the Registration Center (RC) by producing a secret number that isn't stored in the phone, which protects against privileged insider attacks. The user and server generate a nonce for dynamic user identity and agree on a session secret key for safe communication. The passwords are not stored on the computer or provided in plain text, they are resistant to replay, guessing, and stolen verification attacks. The suggested protocol uses a one-way hash function and XOR operations, with the client having remote access to a large number of servers over a secure communication channel. Concentrates on HMAC and SHA3 for Collision Free Hashing and to overcome length extension attacks. HMACs are substantially less affected by collisions than their underlying hashing algorithms alone. So adding an HMAC to an MD5 or SHA hash would make it substantially more difficult to break via a rainbow table.

Keywords: Registration center; SIM; IMEI

1 Introduction

Comprehension and characterizing client verification and approval among cloud Actors is another basic component of cloud engineering. The information housed by a cloud Ecosystem is not secured by cloud Actors [1]. Cloud customers decide a suitable cloud engineering and organization model to comprehend who are the clients, what information they are attempting to access and how the information is put away.

Authentication of the user is the process of identifying the user, by allowing them to enter the valid username and password (key). The user is authorized by the authorization server by comparing the user stored credentials at the database [2]. If the user credentials match then the client has benefits to get to the cloud administrations. If the user identifications do not match then the user is not permitted to access the cloud services.

Location-based authentication is a type of authentication given to a user based on the geographical location of the user. If there is a cloud customer in the U.S. and the user wishes to access the cloud services via a Web application or browser in his personal computer, the users are allowed to enter their credentials [3].

But in the background, the system verifies the geo-location and IP address, etc. If the user moves to another location the system identifies contrasting geo-location. After receiving the information from the user's device, the program receives additional information for the next authentication stage before the identity is validated.

Implementing rules such as how a user should access resources or facilities is the key component of user authorisation. It comes within the context of user authorization. An authorized user can access various cloud system services providing user authorization is applied to each aspect of a cloud ecosystem's lowest common denominator. Ensuring data security within the cloud information system is important [4]. It can undermine a program by giving users more power than they need. Protecting user information from the centre is important and must be incorporated in a security authorisation program's security policies.

Execution of approval approaches is troublesome in a cloud framework. The client validation and approval server can execute the arrangements. The cloud foundation design is answerable for dealing with the application and verifying and supporting clients. The cloud infrastructure architecture is in control of managing, authenticating and approving users [5]. Cloud clients need to choose the best answer for their cloud framework, as client validation and approval procedures, strategies and systems are fundamental to making sure about their information in a cloud environment.

As technological advances as a standardized solution for fulfilling the operational needs of many organizations forms as cloud computing. There are different methods to authenticate users in the cloud environment, such as username and password, Mobile Trusted Module (MTM), Single Sign on (SSO), multifaceted confirmation, Public Key Infrastructure (PKI), just as biometric verification. This study proposes a key agreement protocol scheme for user authentication in the mobile cloud environment [6].

1.1 Mutual Authentication System

Industry and academia are more concerned about the concept of cloud computing. Cloud computing security has become a vulnerability hotspot, which is the main concern of current users worldwide regarding cloud computing [7]. To access the cloud services the cloud computing service centre is used to store and process the user credentials. The safety of the cloud computing system is affected if any private information is leaked or lost. To transmit data among clients and the server and ensure a private correspondence channel is required. In authentication, Identity is the cornerstone of the complete security architecture and the core technique for maintaining cloud computing system security [8].

For secure communication between users and servers, both entities have to authenticate each other by providing their identities. A secure private communication channel is created after the client proves his identity to the server and vice versa [9]. This method is broadly used by clients, as it helps to reduce online threats. Mutual Authentication is an effective tool for creating a stable client-server connection.

A discreet result of mutual authentication provides a secure channel to protect data from various online frauds such as denial of service and many more [10].

1.2 User Authentication System

In network security trusted computing technology has developed. In trusted cloud computing a sort of smart card password authentication is proposed [11]. This provides a secure communication channel for generating a final session key and guarantees the reality of cloud servers and user individualities and lets genuine users check the reliable position of the cloud server. It can also efficiently address the problem of uniqueness of the user in authentication and secure transmission between the server and the user in the cloud environment [12].

In the field of medicine, trustworthy protection schemes in cloud computing are crucial. The current medical system is introducing online services and digital technology to treat patients worldwide [13]. The use of MR images in brain tumour detection has been analysed in recent research [14]. The process for safe transmission of MR images through a cloud system has been shown.

2 Related Works

A data security model that includes OTP generation for user authentication using HMAC (Hash-based message authentication code). It gives a comparative study of MD5 and SHA algorithms. This uses encryption algorithms to transform the original text into a hashed form that the third party can not anticipate. Eventually, Data quality can be seen as a major problem, which is seen as a threat to the cloud environment [15]. The proposed model typically replicates our data and stores it in different locations to overcome this problem.

The concept of a less public key cryptography certificate, which lies between identity-based approaches with the traditional PKI [16]. The concept is built from linear maps. This paper exposed about the appropriate model of the CL-PKE scheme is stable, assuming the Generalized Bilinear Diffie Hellman Problem (GBDHP) is difficult [17].

The various authentication methods to verify the user before granting access to resources has been analysed [18]. And also analysed authentication techniques together with the existing methods. Pron and Cons of each method are analysed to aware the experts who use the cloud services up to a maximum level [19].

It provides an overview of cloud computing, components (the cloud infrastructure and cloud applications [20] and discusses the problems of cloud computing in mobile applications and their possible solutions. A new authentication system for mobile customers using certified public keys by the user [21]. The mobile client was able to change the password with the registration center and analysed that the system will withstand different possible multi-server attacks.

The novel approach in the multi-server environment with an authenticated key agreement using smart cards with an efficient password [22]. The effective upgrade of greater security over Liao – Wang's scheme [23]. The enhanced scheme's stability, productivity and computational costs are well adapted to the practical application environment.

A protocol that would be practical and computationally efficient to implement. It only uses nonce, one-way hash functions are used with XOR operations in the implementation [24]. A protected method is proposed for the modification of the user credentials. The dynamic id based authentication was proposed for a multi-server environment [25]. The cloud user id can be changed dynamically and the session key is generated for further communication [26–28].

3 Proposed Authentication Protocol

The authentication protocol suggested the following participants are considered to be present. The Centre for Registration (RC), Ui and Sj Server. The proposed procedure consists of three different stages,

- User Registration,
- Login Stage
- Authentication Stage

3.1 Registration Phase

As per the assumption given above, Ui’s registration with the RC is a one-time operation carried out via private communication through a secure channel.

Step 1: U_i chooses an identity ID_i, Password PW_i and generates a random number b to compute $A_i = h(ID_i \oplus b \oplus PW_i)$. Ui then transmits IDi and Ai via the protected private communication channel to the RC for registration purposes.

Step 2: The RC computes $B_i = h(A_i \| x)$, $C_i = h(ID_i \| h(y) \| A_i)$, $D_i = h(B_i \| h(x\|y))$, and $E_i = B_i \oplus h(x\|y)$. The RC stores $\{C_i, D_i, E_i, h(y), h(.)\}$ on the User’s smart phone.

Step 3: Now U_i computes $L_i = b \oplus h(IMEI \| SIM \|ID_i \| PW_i)$ and keys L_i into the smartphone. Now the phone contains the following details $\{C_i, D_i, E_i, L_i\ h(y), h(.)\}$. Here the secret random number b is not stored in the phone, instead, it computes L_i and This helps us counter the privileged assault on the attack.

The above steps are shown in Fig. 1.

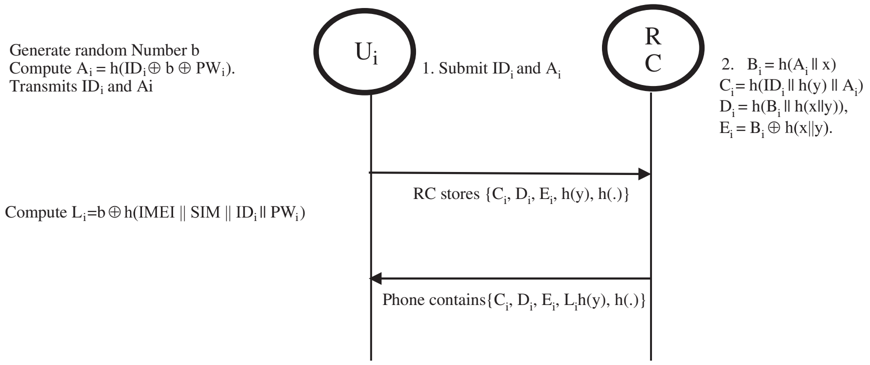
Generate random Number b
Compute $A_i = h(ID_i \oplus b \oplus PW_i)$.
Transmits ID_i and Ai
U_i
1. Submit ID_i and A_i
R
C
2. $B_i = h(A_i \| x)$
$C_i = h(ID_i \| h(y) \| A_i)$
$D_i = h(B_i \| h(x\|y))$,
$E_i = B_i \oplus h(x\|y)$.
RC stores $\{C_i, D_i, E_i, h(y), h(.)\}$
Compute $L_i = b \oplus h(IMEI \| SIM \| ID_i \| PW_i)$
Phone contains$\{C_i, D_i, E_i, L_i h(y), h(.)\}$

Figure 1: Registration phase

3.2 Login Phase

Here the User sends the Server a login request message.

Step 1: Uses the smartphone to initiate the login process by inputting the ID_i and the PW_i.

Step 2: The smartphone performs the computation $b = Li \oplus h(IMEI \| SIM \| ID_i \| PW_i)$. It computes $A_i = h(ID_i \oplus b \oplus PW_i)$ and $C_i = h(ID_i \| h(y) \| A_i)$ and matches whether the computed value C_i^* matches with the C_i which is already available in the smartphone. If there is no match the session will be aborted.

Step 3: If match is found the smart phone will generate a nonce N_i based on the IMEI and the SIM number. The phone then computes $CID_i = A_i \oplus h(D_i \| SID_j \| N_i)$, $P_{ij} = E_i \oplus h(h(SID_j \| h(y) \| N_i)$, $M_1 = h(P_{ij} \| CID_i \| A_i \| N_i)$, and $M_2 = h(SID_j \| h(y)) \oplus N_i$.

Step 4: User U_i sends a login request message $\{CID_i, P_{ij}, M_1, M_2\}$ to S_j via a public channel.

The above steps are shown in Fig. 2.

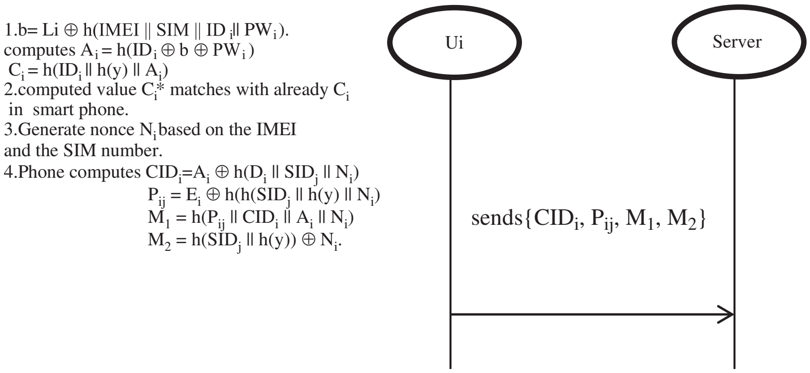
1.b= Li ⊕ h(IMEI || SIM || ID $_i$|| PW$_i$).
computes $A_i = h(ID_i \oplus b \oplus PW_i)$
$C_i = h(ID_i \| h(y) \| A_i)$
2.computed value C_i* matches with already C_i
in smart phone.
3.Generate nonce N_i based on the IMEI
and the SIM number.
4.Phone computes $CID_i=A_i \oplus h(D_i \| SID_j \| N_i)$
$P_{ij} = E_i \oplus h(h(SID_j \| h(y) \| N_i)$
$M_1 = h(P_{ij} \| CID_i \| A_i \| N_i)$
$M_2 = h(SID_j \| h(y)) \oplus N_i$.
Ui
Server
sends{CID_i, P_{ij}, M_1, M_2}

Figure 2: Login phase

3.3 Authentication and Key Agreement Phase

The steps to validate the login request and calculate the shared authentication challenge-response message must take by the server and the user, and both will settle on a SKeyij session secret key for further secure communication.

Step 1: The server S_j computes $N_i = h(SID_j \| h(y)) \oplus M_2$, $E_i = P_{ij} \oplus h(h(SID_j \| h(y)) \| N_i)$, $B_i = E_i \oplus h(x \| y)$, $D_i = h(B_i \| h(x \| y))$, $A_i = CID_i \oplus h(D_i \| SID_j \| N_i)$ using the message credentials {P_{ij}, CID_i, A_i,N_i} and the known credentials $h(x \| y)$, $h(y)$.

Step 2: S_j computes $h(P_{ij} \| CID_i \| A_i \| N_i)$ and matches it with M_1. If it doesn't match the server won't accept the request and stop the session. The login request message is accepted and a nonce is created N_j. S_j computes $SK_{ij} = h(h(B_i \| h(x \| y)) \| A_i)$, $M_3 = h(SK_{ij}, \| A_i \| SID_j \| N_j)$ and $M_4 = SK_{ij} \oplus N_j$. Next the Server S_j sends the message {M_3, M_4} to U_i via a public communication channel.

Step 3: After received {M_3, M_4} from S_j, the user U_i computes $SK_{ij} = h(D_i \| A_i)$, and extracts the nonce N_j by computing $N_j = SK_{ij} \oplus M_4$ and checks whether $h(SK_{ij} \|A_i \|SID_j \| N_j)$ is equal to M_3. If they are found to be equal, U_i successfully authenticates S_j. Further U_i computes $M_5 = h(SK_{ij}, \| A_i \| SID_j \| N_i \| N_j)$ and sends the message {M_5} to S_j via a public channel. If it doesn't match, the session is terminated.

Step 4: Sj calculates h(SKij,) and compares it to M5. If they match, the mutual authentication will be complete. Now they will both compute a common secret session key $SKey_{ij} = h(SK_{ij}, \| A_i \| SID_j \| N_i \| D_i \| N_j)$ for their secure future communication.

Further, if there is any need to change the Password or Device (IMEI) or SIM, then the user must provide a request from the smartphone by providing the current credentials and the new credentials and compute a new value for $L_{inew} = b \oplus h(IMEI_{new} \| SIM_{new} \| ID_i \| PW_{inew})$ and key in the L_{inew} into the smartphone for further authentication [24]. The protocol authentication information is being shown in Fig. 3.

3.4 Hash-Based Message Authentication Code

Here we can concentrate on HMAC and SHA3 for Collision Free Hashing and overcome length extension attacks. HMACs are less affected by collisions than their underlying hashing algorithms alone. So adding an HMAC to an MD5 or SHA hash would make it substantially more difficult to break via a rainbow table. Further, HMAC is not susceptible to length extension attacks. Tab. 1 shows a Comparison of Hash functions and Their Collision and Security Features. Tab. 2 shows the Comparison of Security Features.

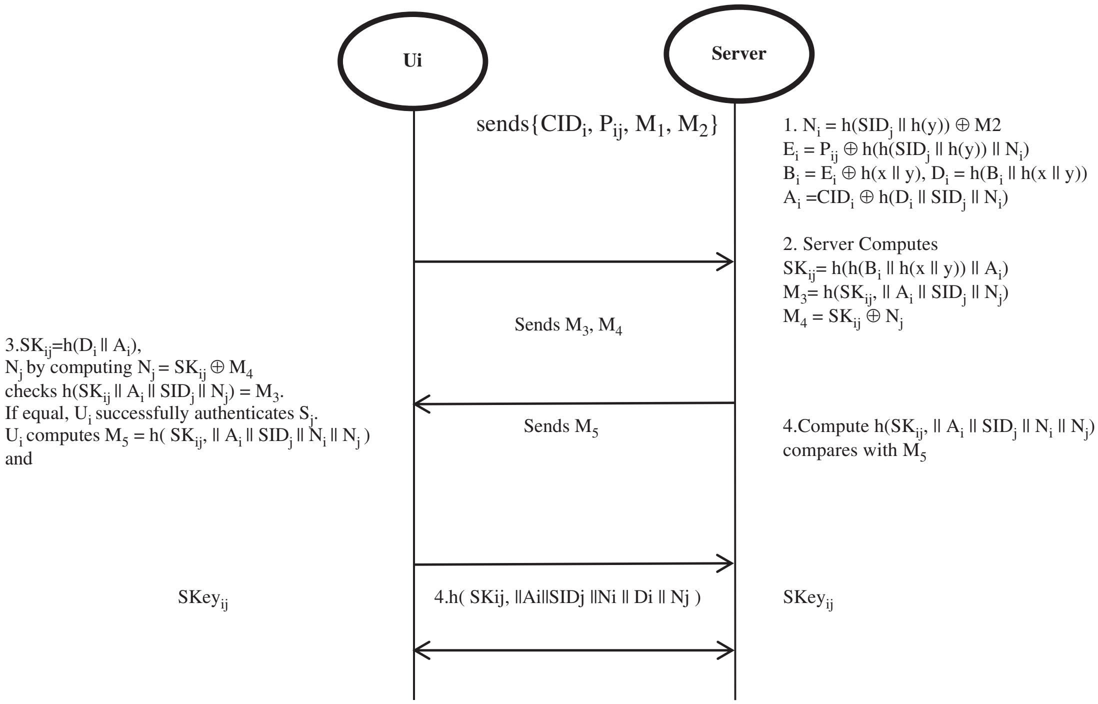
Ui
Server
sends$\{CID_i, P_{ij}, M_1, M_2\}$
1. $N_i = h(SID_j \| h(y)) \oplus M2$
$E_i = P_{ij} \oplus h(h(SID_j \| h(y)) \| N_i)$
$B_i = E_i \oplus h(x \| y)$, $D_i = h(B_i \| h(x \| y))$
$A_i = CID_i \oplus h(D_i \| SID_j \| N_i)$
2. Server Computes
$SK_{ij} = h(h(B_i \| h(x \| y)) \| A_i)$
$M_3 = h(SK_{ij}, \| A_i \| SID_j \| N_j)$
$M_4 = SK_{ij} \oplus N_j$
Sends M_3, M_4
3.$SK_{ij}=h(D_i \| A_i)$,
N_j by computing $N_j = SK_{ij} \oplus M_4$
checks $h(SK_{ij} \| A_i \| SID_j \| N_j) = M_3$.
If equal, U_i successfully authenticates S_j.
U_i computes $M_5 = h(SK_{ij}, \| A_i \| SID_j \| N_i \| N_j)$
and
Sends M_5
4.Compute $h(SK_{ij}, \| A_i \| SID_j \| N_i \| N_j)$
compares with M_5
$SKey_{ij}$
4.h(SKij, ||Ai||SIDj ||Ni || Di || Nj)
$SKey_{ij}$

Figure 3: Authentication and key agreement phase

Table 1: Comparison of hash functions and their collision and security features

Algorithm	Output size (bits)	Block size (bits)	Rounds	Operations	Security (in bits) against collision attacks	Capacity against length extension attacks
MDS	128	512	54	and, XOR, add, *mod* 2^{32}, OR	=18 (collisions found)	0
SHA-0	160	512	80	and, XOR, add, *mod* 2^{32}, OR	<34 (collisions found)	0
SHA-1	256	512	64	and, XOR, rot, add, *mod* 2^{32}, or, shr	<63 (collisions found)	0
SHA-3 256	256	1088	24	and, XOR, rot, not	128	512

4 Security Analysis

4.1 Efficient Mechanism for Password Verification

In the Scheme proposed, the feedback of the user can be checked effectively. The correct credentials like ID, Password, etc. Also, it is possible to make sure that the login request is sent from the authorized device using the approved mobile number, as we are utilizing IMEI and SIM to calculate L_i which is in turn used to compute b. If the computed C_i* doesn't match with C_i stored in the phone then the request will be rejected and the session terminated. This allows the proposed protocol to verify the credentials effectively

Table 2: Comparison of security features in the proposed protocol

S. no	Security attributes	Al-Riyami et al. [1]	Wang et al. [2]	Sahu et al. [3]	Yi et al. [4]	Proposed model
1	Password guessing attack	No	No	No	No	Yes
2	Privileged insider attack	Yes	Yes	Yes	Yes	Yes
3	User anonymity	Yes	Yes	Yes	Yes	Yes
4	Stolen card/device attack	Yes	No	No	No	Yes
5	Impersonation attack	No	No	No	No	Yes
6	Replay attack	Yes	Yes	Yes	Yes	Yes
7	Proper mutual authentication	No	No	No	No	Yes
8	Good repairability	No	No	No	No	Yes
9	Forgery attack	No	No	No	No	Yes
10	Two factor security	No	No	No	No	Yes
11	Session key agreement	Yes	Yes	Yes	Yes	Yes
12	Efficient password change	Yes	No	Yes	Yes	Yes
13	Collision free hash function	No	No	No	No	Yes
14	Length extension attack	No	No	No	No	Yes

4.2 User Anonymity

In the proposed protocol for authentication, the server received from the user as a login entry and that doesn't contain the user ID since the ID_i sent to the server is computed for every session dynamically. Thus the anonymity of the user U_i is preserved. That parameter is related to a nonce is kept securely through the hash function that makes that process dynamic.

4.3 Stolen Phone/Device Attack

If the User U_i's mobile device is stolen or lost. The hacker can extricate the put-away information {Ci, Di, Ei, Li, h(y), h(.)} from the telephone. But still, the adversary cannot make use of this information as the adversary still lacks the user ID (ID_i) and the password (PW_i). It is presumed that the opponent cannot simultaneously guess both the ID and the password, and that they are also protected by one type of hashing functions. Further, the user can block the SIM and IMEI and hence the adversary cannot receive the OTP and hence the proposed protocol provides protection against stolen phone/device attacks.

4.4 Password Guessing Attack

This scheme is capable of withstanding password predicting attacks as the user U_i needs to input both the ID and Password into the device during a login request. Calculated values like b, Ai, and Ci * are also provided by a one-way hashing function. Further, the additional dependency on IMEI and SIM coupled with the OTP process makes it difficult to do a brute force guessing attack.

4.5 Replay and the Middle Attacks

The use of the two Ni nonce numbers generated by the user device (depending on IMEI and SIM) and the server-generated Nj will keep All messages for that session are dynamic and valid only. and hence it is impossible to do a replay attack. Further, even if the adversary captures the previous login request, without the N_i, D_i and A_i, it is not possible to compute M_5. Further, the IMEI and SIM numbers are obtained from the device directly, The opponent cannot calculate b. The authentication will therefore fail and The proposed protocol offers effective protection against replay and man attacks in the centre.

4.6 Forgery Attack

The attacker can eavesdrop to fool the server with a legitimate login request. The opponent will not be able to create a legitimate login request-response even if it is done without understanding Ei, Ai, Di and Ni. Since it requires the IMEI and SIM numbers as well, the adversary can't do it from another device. Even if the device of the user is stolen, without the Password and ID the attacker won't be able to request a server login message. Thus the proposed protocol can withstand forgery attacks.

4.7 Spoofing Attacks on Servers and Registration Centres

If the attacker is a legal but malicious insider, or if the opponent is a legal system server, they cannot masquerade other server's secret information $h(SID_j \parallel h(y))$ and without that, the challenger cannot compute a valid response message $\{M_3, M_4\}$. Further, the dependency on the device IMEI and SIM make the process further complicated and impossible.

4.8 Known Key Secrecy

Any other session keys should not be compromised. In the proposed model the nonce N_i and N_j and the need for SK_{ij}, D_i, and A_i, makes it impossible to obtain other keys. Also, all these keys are hashed by one-way hash functions. The proposed protocol is immune to known key secrecy attacks.

4.9 Forward Secrecy

In the proposed protocol, by understanding the IDi, Password PWi, random key b, the opponent cannot compute any session key. Thus the proposed model maintains forward secrecy effectively.

4.10 Service Denial Attack

In this method, the server verifies the user's legitimacy and once checked, the mutual authentication is done between the server and the user and this model is therefore protected against this type of attack.

4.11 Good Reparability

One of the most desirable features of a strong security system is its Reparability. It is the ability to revoke a lost or stolen phone or device. In this case, the user has the option to block the SIM and the IMEI number and without the knowledge of ID_i and Password PW_i, the adversary will not be able to make use of the information in that device. The proposed model is further guaranteeing user anonymity and resists stolen device attacks and hence is considered to be a model with good reparability.

5 Conclusion

The proposed authentication scheme is a robust user authentication for a cloud environment. The main advantages of this scheme are the Registration of one-time users at the registration centre to use the services from appropriate servers. The proposed work does not store the user credentials at the server. The passwords can be chosen by the users and can change if needed. The cost of computing and transfer the message is very low. The session key is used for mutual authentication between server and client. The scheme proposed is a nonce-based scheme that has no serious time synchronization problem and nonce is created using the mobile client's IMEI and SIM number. The scheme satisfies all essential requirements. The scheme will withstand any potential attacks in the cloud environment. The above scheme is well suitable for mobile devices to improve their performance with fewer energy resources and computational capabilities.

Acknowledgement: We show gratitude to anonymous referees for their useful ideas.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," In: Laih CS. (eds) in *Advances in Cryptology-ASIACRYPT 2003 Lecture Notes in Computer Science*, vol. 2894. Berlin, Heidelberg: Springer, 2003.

[2] C. Wang, X. Zhang and Z. Zhiming, "Cryptanalysis and improvement of a biometric-based multi-server authentication and key agreement scheme," *Plos one*, vol. 11, no. 2, 2016. https://doi.org/10.1371/journal.pone.0149173.

[3] D. Sahu, S. Sharma, V. Dubey and A. Tripathi, "Cloud computing in mobile applications," *International Journal of Scientific and Research Publications*, vol. 2, no. 8, pp. 1–9, 2012.

[4] G. Yi, Y. A. Heo, H. Byun and Y. S. Jeong, "MRM: Mobile resource management scheme on mobile cloud computing," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 4, pp. 1245–1257, 2018.

[5] H. Shen, C. Gao, D. He and L. Wu, "New biometrics-based authentication scheme for multi-server environment in critical systems," *J Ambient Intell Human Computing*, vol. 6, pp. 825–834, 2015.

[6] H. C. Hsiang and W. K. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for the multi-server environment," *Computer Standards & Interfaces*, vol. 31, no. 6, pp. 1118–1123, 2009.

[7] H. Farooq, "A review on cloud computing security using authentication techniques," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 2, pp. 19–22, 2017.

[8] W. C. Ku and S. M. Chen, "Weaknesses and improvements of an efficient password-based remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 204–207, 2004.

[9] C. C. Lee, Y. M. Lai and C. T. Li, "An improved secure dynamic ID-based remote user authentication scheme for multi-server environment," *International Journal of Security and Its Applications*, vol. 6, no. 2, pp. 203–210, 2012.

[10] X. Li, J. Ma, W. Wang, Y. Xiong and J. Zhang, "A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments," *Mathematical and Computer Modelling*, vol. 58, no. 1–2, pp. 85–95, 2013.

[11] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu *et al.*, "Authentication in the clouds: A framework and its application to mobile users," in *Proc. of ACM Workshop on Cloud Computing Security Workshop*, Chicago Illinois, USA, pp. 1–6, 2010.

[12] S. K. Sood, A. K. Sarje and K. Singh, "A secure dynamic identity-based authentication protocol for multi-server architecture," *Journal of Network and Computer Applications*, vol. 34, no. 2, pp. 609–618, 2011.

[13] S. Gokulakrishnan and J. M. Gnanasekar, "Data integrity management for detection of redundancy and recurrence patterns in cloud," *Journal of Ambient Intelligence and Humanized Computing*, 2019. https://doi.org/10.1007/s12652-019-01530-9.

[14] S. Sneha, L. Nath and M. Gladence, "Security for bicycle and investigation of health of bicycle rider using IoT," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 16, pp. 1298–1303, 2017.

[15] S. M. Shetty and S. Shetty, “Analysis of load balancing in cloud data centres,” *Journal of Ambient Intelligence and Humanized Computing*, 2019. https://doi.org/10.1007/s12652-018-1106-7.

[16] W. S. Juang, “Efficient multi-server password authenticated key agreement using smart cards,” *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 251–255, 2004.

[17] X. Li, Y. Xiong, J. Ma and W. Wang, “An efficient and security dynamic identity-based authentication protocol for multi-server architecture using smart cards,” *Journal of Network and Computer Applications*, vol. 35, no. 2, pp. 763–769, 2012.

[18] Y. P. Liao and S. S. Wang, “A secure dynamic ID based remote user authentication scheme for the multi-server environment,” *Computer Standards & Interfaces*, vol. 31, no. 1, pp. 24–29, 2009.

[19] Y. P. Liao and C. M. Hsiao, “A ovel multi-server remote user authentication scheme using self-certified public keys for mobile clients,” *Future Generation Computer Systems*, vol. 29, no. 3, pp. 886–900, 2013.

[20] Y. H. Chuang and Y. M. Tseng, “CAKE: Compatible authentication and key exchange protocol for a smart city in 5G networks,” *Symmetry*, vol. 13, no. 4, pp. 698, 2021.

[21] P. Sudhakaran, S. Swaminathan, D. Yuvaraj and S. S. Priya, “Load predicting model of mobile cloud computing based on glowworm swarm optimization LSTM network,” *International Association of Online Engineering*, vol. 14, no. 5, pp. 150–163, 2020.

[22] D. Yuvaraj, N. R. Dharunyaa, S. Nandhini,V. Priyadharshini and A. Supriya, “Enhanced data security through data integrity on cloud computing,” *International Journal of Pure and Applied Mathematics*, vol. 118, no. 22, pp. 1079–1083, 2018.

[23] B. Bazeer Ahamed, D. Yuvaraj and V. Manikandan, “Computation of testing approach in cloud mobility service,” *International Journal of Cloud Computing*, vol. 10, no. 1/2, pp. 158–177, 2020.

[24] B. B. Ahamed and D. Yuvaraj, “Dynamic secure power management system in mobile wireless sensor network,” in *Int. Conf. on Intelligent Computing & Optimization*, Thailand, Springer, pp. 549–558, 2018.

[25] D. Yuvaraj, M. Sivaram, A. Mohamed Uvaze Ahamed and S. Nageswari, “Some investigation on DDOS attack models in mobile networks,” *International Journal of Interactive Mobile Technologies*, vol. 13, no. 10, pp. 71–88, 2018.

[26] S. Shanmugapriya, A. Valarmathi and D. Yuvaraj, “The personal authentication service and security enhancement for an optimal strong password,” *Concurrency and Computation: Practice and Experience*, vol. 31, no. 13, pp. 5009–5014, 2018.

[27] S. J. Hussain, U. Ahmed, H. Liaquat, S. Mir, N. Jhanjhi and M. Humayun, “IMIAD: Intelligent malware identification for android platform,” in *Int. Conf. on Computer and Information Sciences (ICCIS)*, Saudi Arabia, 2019.

[28] Z. A. Almusaylim and N. Z. Jhanjhi, “Comprehensive review: Privacy protection of user in location-aware services of mobile cloud computing,” *Wireless Pers Commun*, vol. 111, pp. 541–564, 2020.