JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 33, 727-741 (2017)
DOI: 10.6688/JISE.2017.33.3.8

An Efficient Authentication Scheme for Mobile Cloud Computing Services

SIVARAMAN AUDITHAN[1,*], VIJAYAREGUNATHAN VIJAYASARO[2],
PANDI VIJAYAKUMAR[3] AND VARADARAJAN VIJAYAKUMAR[4]
[1]*Department of Electronics and Communication Engineering*
P.R. Engineering College
Thanjavur, 613403 India
[2]*Department of Electronics and Communication Engineering*
PRIST University
Thanjavur, 613403 India
[3]*Department of Computer Science and Engineering*
University College of Engineering Tindivanam
Melpakkam, Tamilnadu, 604001 India
[4]*School of Computing Science and Engineering*
VIT University
Chennai Campus, 600127 India
E-mail: {saudithan; viji.saro17; vijibond2000}@gmail.com; vijayakumar.v@vit.ac.in

The explosive growth of mobile users has been increasing in the past few years. In this paper, an efficient authentication scheme for distributed mobile cloud computing is proposed. This proposed scheme enables the users to access multiple service providers with a single private key. Instead of opting traditional public key cryptosystem like RSA, the proposed scheme uses bilinear pairing technique for effective anonymous authentication. This scheme supports mutual authentication. In our proposed scheme, mobile cloud users and service providers are only allowed to communicate during the authentication process. The third party is considered to be trusted and it participates in the registration of mobile cloud users and the service providers. In addition, our proposed scheme prevents the malicious mobile users and service providers through the third party revocation mechanism. With this design, our proposed scheme reduces the computation cost during the anonymous mutual authentication between the mobile cloud user and the service provider. Performance analysis is conducted to show that our proposed scheme is computationally efficient in comparison with the previously used schemes in the literature.

Keywords: anonymous authentication, mobile cloud, bilinear pairing, computation cost, message integrity

1. INTRODUCTION

Cloud computing is a type of computing where storing and accessing of data and other programs are done outside the computer through the Internet rather than using the computer's hard drive. In other words, cloud computing is the third party data centers where the users can store and access their data with various capabilities. It is used to share the computing resources rather than using personal devices or local servers to handle applications. Mobile cloud computing is the combination of mobile computing, cloud computing and also wireless networks to provide better computational resources to the

Received July 16, 2016; revised August 16, 2016; accepted August 21, 2016.
Communicated by Balamurugan Balusamy.

mobile users and also for the network operators. It is the simplest infrastructure where storing and processing of the data will happen outside the mobile device. It will allow the users to access the services anywhere whenever it needs through the Internet. It is based on the principle "pay as you use". Most commonly used mobile computing devices are portable computers, mobile phones, wearable computers and smart cards. Mobile cloud computing allows the users to access software and platforms at low cost. Allowing the users to store and process the data outside the mobile device will help to increase the configuration speed of the device. It will allow universal access to the services. It will provide the software and platforms up to date and provide flexibility to access. It will extend the battery life of mobile phones. It will also provide better bandwidth and leads to have a good storage capacity. Data storing capacity and processing power will be increased when we use the mobile cloud computing. Regarding the popularity of mobile cloud computing, the study of ABI research done in the year 2015 concludes that accessing the cloud services through the mobile devices for the business purpose increases more than 240 million. This will move the income of mobile cloud computing to reach 5.2 billion [1].

The important issue in mobile cloud computing is the security. The service providers of the cloud must support secure and efficient authentication schemes to avoid illegal access. The authentication is the first level of defense against all attacks. It will prevent the illegal access by adversaries or unauthorized users. There are many existing authentication schemes [2-4] used for mobile cloud computing which should solve the three following concerns. First important issue is the computational overhead, since the mobile devices have limited capability of computing when compared with the computers or laptops. Hence, the efficiency of computing must be seriously considered. The second issue is the strength regarding security. Since the messages are transmitted over an insecure Wireless Local Area Network (WLAN), there is a chance for an adversary to interrupt or modify the transmitted message before they reach the correct recipient. The final thing is that the masquerader has the chance to access the resources instead of the original recipients. So, the privacy protection is must [3, 4] for the account of each user. These things should be resolved during the time of authentication. Moreover, another important challenging issue in most of the existing schemes is key management. A single user is in the position to access different services from more than one service provider. In these scenarios, users are interested to access multiple services from various service providers through the single private key. Therefore, designing an effective data access scheme using a single private key is necessary.

1.1 Our Contributions

Based on the above mentioned challenges, the main contributions of this paper are summarized as follows.

1. To propose a computationally efficient anonymous mutual authentication scheme for mobile cloud users to verify the authenticity of the users without revealing their real identities to the Service Provider (SP).
2. To provide data integrity during message transmission which is suitably required for mobile cloud computing.

3. To provide a conditional tracking mechanism through which the third party (TP) traces the misbehaving Service Provider (SP) that abuses the mobile cloud computing. Thus, a TP can revoke privacy of the misbehaving SPs from causing any further damage.
4. To propose an efficient authentication scheme to anonymously authenticate the SPs before getting information from it.

1.2 Roadmap

The remaining sections of this paper are organized as follows. Section 2 summarizes the related works. The system model and preliminaries are given in section 3. We describe our proposed anonymous authentication schemes in section 4. We present the security analysis in section 5. Section 6 gives performance evaluation of our proposed scheme. Section 7 provides the conclusion of this paper.

2. RELATED WORKS

In the field of authentication and privacy of mobile cloud computing, the bulk of the research works [20-25] have concentrated on authentication to guarantee the security. In all these existing works, ID-based authentication schemes were used. The main limitation of these existing schemes is that the privacy is not protected during the time of authentication which leads to privacy-related attacks. W. S. Juang *et al.* [5] proposed an authenticated key agreement mechanism using smart cards. This scheme is used to protect the identity information during authentication. The security of this system is based on symmetric cryptosystem and the elliptic curve cryptosystem. However, the scheme has the following disadvantages. This scheme doesn't provide a password changing mechanism and user untracebility. Also, the generation and distribution of session key was a difficult task. L. Chen *et al.* [6] proposed ID based authenticated key agreement protocol scheme to provide mutual authentication and key exchange mechanism. The major drawback of this scheme is high computational cost. D. Giri and Srivastava [7] proposed efficient ID based remote user authentication scheme. This scheme has the ability to withstand forgery attack. In contrast, this scheme doesn't support mutual authentication and key exchange. In addition, the computation cost is also high. Authenticated key agreement protocol is also used in various papers [8-10]. It will provide the mutual authentication and key exchange mechanism. The important drawback is that high computational cost.

T. Eissa *et al.* [11] proposed an RSA public authentication scheme which is named as Ron Rivest, Adi Shamir and Leonard Adleman (ID-RSA). Only the trusted entities are allowed to access the public key of the users through which it can withstand RSA cryptanalysis. Since bilinear pairing is used, the cost of computation tends to be high. H. S. Rhee *et al*. [12] proposed a secured user authentication scheme which uses a USB stick instead of smart cards. This scheme uses modular exponentiation and multiplication operations which are unable to be applied in remote user authentication using the mobile devices which have less computing power. Another disadvantage is that it is unable to withstand from the impersonation attack.

M. L. Das *et al*. [13] proposed remote user authentication scheme with smart cards. This scheme uses the bilinear pairing operation. It can handle forgery attack and insider attack. Simultaneously, it lacks mutual authentication and session key agreement. Moreover, there is more possibility for the replay attack. M. S. Hwang and L. H. Li [14] proposed a password authentication protocol without using password tables. Without the involvement of password tables, the passwords are authenticated, which in turn provides the resistance against the stealing verifier table attack. The computational cost is high as it uses the public key cryptosystem.

X. J. Tian *et al*. [8] proposed analysis and improvement of ECC based authenticated key exchange protocol. This scheme is able to generate a shared session key through the certificate authority center. The major drawback is that this scheme needs a large space to store all user's public key and also to certify which is inefficient. G. Yang and chang [10] proposed ID based remote mutual authentication with key agreement scheme on ECC for remote devices. This scheme is more efficient. But the main disadvantage is that the authentication is performed without protecting the password which may lead to impersonation attack and insider attack. C. Tang *et al*. [9] proposed an efficient mobile authentication scheme for wireless network. In this scheme a temporary ID is created dynamically for user by the onetime alias mechanism for providing security to the users. The drawback of this scheme is that user id does not support user unlinkability. J. Z. Lu and J. Zhou [15], proposed a delegation based mobile authentication protocol in which the original ID is replaced by a user alias mechanism during the authentication process. The main limitation of this scheme is that it is not able to resist Denial of Service (DoS) Attack.

Comparing with most of the authentication and privacy preserving schemes existing in the literature, we propose an anonymous authentication scheme for mobile cloud computing which anonymously authenticates the mobile cloud users and service providers in a computationally efficient way to preserve the real identities of mobile users and service providers from other entities in the network.

3. SYSTEM MODEL AND PRELIMINARIES

In this section, we demonstrate the system model and the definitions of bilinear pairing.

3.1 System Model

The system architecture of the proposed scheme is shown in Fig. 1. In this system model, the trusted third party (TP) chooses its own master private key and then computes its corresponding public key. During the time of registration, the mobile user and the service provider sends their identities and necessary parameters to the TP. After the successful completion of the registration process, the TP computes the private key and the corresponding public keys along with the necessary authentication parameters for both the user and the service provider and sends back to them in a secure way. After receiving the authentication parameters from the TP the users and the service providers computes its own authentication parameters for anonymous authentication. If the user wants to

communicate with the service provider he/she sends request to the service provider. After the request has been received, the service provider anonymously authenticates the mobile user to avoid communication with the illegal user. Similarly, the mobile user anonymously authenticates the SP before making access to it.

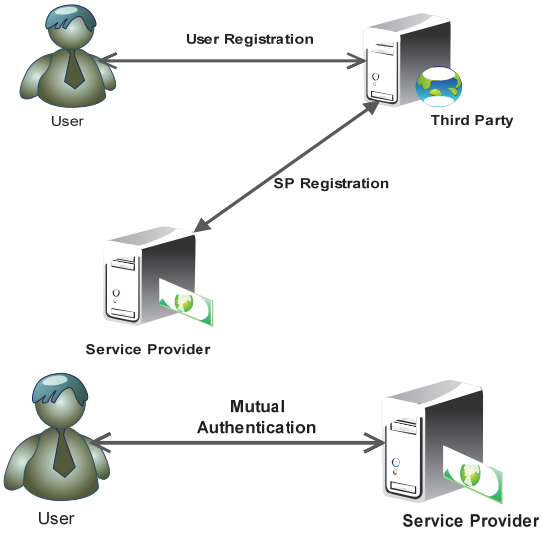

Fig. 1. Process of anonymous authentication scheme for mobile cloud computing environment.

3.2 Bilinear Pairing

Let G_1, G_2 and G_T denote three multiplicative cyclic groups of order q, where q is a large prime. Suppose that G_1, G_2 and G_T are equipped with pairing. The bilinear map e: $G_1 \times G_2 \rightarrow G_T$ satisfies three properties.

1. Bilinearity: The mapping e: $G_1 \times G_2 \rightarrow G_T$ is said to be bilinear if $e(g_2^a, g_2^b) = e(g_1, g_2)^{ab}$, $g_1 \in G_1$ & $g_2 \in G_2$ and $\forall a, b \in Z_{q'}^*$, where $Z_{q'}^* = [1, \ldots, (q-1)]$.
2. Nondegeneracy: $e(g_1, g_2) \neq 1_{GT}$.
3. Computability: There exists an efficient algorithm to easily compute the bilinear map e: $G_1 \times G_2 \rightarrow G_T$.

We denote the isomorphism by ψ and hence a well computable isomorphism ψ: $G_2 \rightarrow G_1$ is basically required. The group that possesses such a map e is called a bilinear group.

4. PROPOSED ANONYMOUS MUTUAL AUTHENTICATION SCHEME

In this section, we propose a new anonymous mutual authentication scheme for mobile cloud computing to anonymously authenticate both users and service providers with less computational cost. This scheme consists of the following four phases namely system initialization, registration, users anonymous authentication and service providers

anonymous authentication.

4.1 System Initialization

The TP initially generates its private and public keys. To compute its initial parameters, the TP picks $l, s \in Z_q^*$ as its private keys and its master key as $z \in Z_q^*$. Then, the TP computes its corresponding public keys as follows.

$$Y_1 = g_1^{l+s}$$
$$Y_2 = g_2^{\frac{1}{(l+s)z}}$$
$$Y_3 = g_1^{l}$$
$$Y_4 = g_1^{s}$$

4.2 Registration

After the successful registration of the SPs, the TP generates the public and private key pair for each SP. The private key of the SP is $x \in Z_q^*$ and the public parameters of the SP are computed below:

$$y = g_1^{x}$$
$$y_1 = g_1^{-x}$$
$$y_2 = Y_1^{x+z}$$
$$y_3 = Y_3^{-x}$$
$$y_4 = Y_4^{-x}$$

Similarly, after the successful registration of the mobile users, the TP generates the public and private key pair for each mobile user. The private keys of the mobile user are $m, n \in Z_q^*$ and the public parameters are as follows,

$$gm_1 = g_1^{m}, \quad gm_2 = g_1^{-m}$$
$$gm_3 = Y_1^{m+z}, \quad gm_4 = Y_3^{-m}$$
$$gm_5 = Y_4^{-m}, \quad gm_6 = g_2^{\frac{1}{m+n}}$$
$$gm_7 = g_1^{n}$$

Then, the TP generates a fake identity along with secret parameter for each mobile user and service provider after generating these public parameters. The use of computing the fake identities and the secret parameter is to prove the legitimacy of the user or the service provider against the masquerading attack. In order to compute the fake identity (*FID*) for every service provider SP_j, the TP chooses a random number f_1 such that $f_1 \in Z_q^*$ and computes $FID_{SPj} = y_4 \cdot g_1^{f_1}$. The mapping from original identities to fake identities is done just in the TP. Next, TA keeps (FID_{SPj}, $id - SP_j$, $g_1^{f_1}$) in its tracking list, where $id - SP_j$ is the original identity (*id*) of SP_j assigned by the TP at the time of its registration. Then the

value of $g_1^{f_1}$, FID_{SPj} are given to the service provider and these parameters are kept secret by it. Similarly, FID_{Ui} is computed for each user.

4.3 Users Anonymous Authentication

Once the mobile user starts sending the request messages to the service provider, the mobile user needs to check the legitimacy of the SP against masquerading attack. To perform this task, the mobile user sends a request $\{FID_{Ui} \| y_4\}$ which has its fake identity and the one of the public values y_4 of SP_j to the TP. After receiving this, the TP sends $\{FID_{Ui} \| FID_{SPj}\}$ to the mobile user. By receiving this, the mobile user sends a request to the SP for verification. Hence, the SP compute $B = gm_1 \cdot g_1^{f_1}$ and sends it back to the mobile user. Then, the mobile user checks the following condition

$$B \cdot gm_2 \cdot y_4 = FID_{SPj}.$$

***Proof of Correctness*:**

$$\begin{aligned} & B \cdot gm_2 \cdot y_4 = gm_1 \cdot g_1^{f_1} \cdot gm_2 \cdot y_4 \\ & = g_1^{m} \cdot g_1^{f_1} \cdot g_1^{-m} \cdot y_4 \\ & = g_1^{f_1} \cdot y_4 \\ & = FID_{SPj} \end{aligned}$$

If this condition holds, the mobile user considers that service provider is not masqueraded. Because, in order to masquerade to be another entity, it is necessary to know the value f and FID_{SPj}. Since, these two parameters are secret parameters, it is not possible for an intruder to perform the masquerading attack. Moreover, the mobile user needs to check the legitimacy of the public parameters of the SP by checking the following condition before making communication with it.

$$e(y_2 \cdot y_3 \cdot y_4, Y_2) = e(g_1, g_2)$$

***Proof of Correctness*:**

$$\begin{aligned} & e(y_2 \cdot y_3 \cdot y_4, Y_2) = e(Y_1^{x+z} \cdot Y_3^{-x} \cdot Y_4^{-x}, g_2^{\frac{1}{(l+s)z}}) \\ & = e(Y_1^{x} \cdot Y_1^{z} \cdot Y_3^{-x} \cdot Y_4^{-x} \cdot g_2^{\frac{1}{(l+s)z}}) \\ & = e(g_1^{(l+s)x} \cdot g_1^{(l+s)z} \cdot g_1^{-lx} \cdot g_1^{-xs}, g_2^{\frac{1}{(l+s)z}}) \\ & = e(g_1^{(l+s)x} \cdot g_1^{(l+s)z} \cdot g_1^{-x(l+s)}, g_2^{\frac{1}{(l+s)z}}) \\ & = e(g_1^{(l+s)z}, g_2^{\frac{1}{(l+s)z}}) \\ & = e(g_1, g_2)^{\frac{(l+s)z}{(l+s)z}} \\ & = e(g_1, g_2) \end{aligned}$$

If it holds, then the mobile user ensures that the SP is an authenticated one, otherwise the mobile user avoids communication with the illegal SP.

In order to prove the integrity of the sending messages, the service provider picks a

random number as $d \in Z_q^*$. In addition, the SP takes the message *mes* and its corresponding hash function $SHF = H_1(mes)$ and computes

$$c_1 = y \cdot gm_1$$
$$\sigma_1 = c_1 \cdot gm_1$$
$$\sigma_1 = y^d$$
$$\sigma_3 = y_1 \cdot gm_2$$
$$\sigma_4 = y_1^d \cdot gm_7$$
$$\sigma_5 = g_1^{\frac{1}{SHF}}$$

After generating these parameters, the mobile user first generates the hash function $RHF = H_1(mes)$ for the received message and checks whether the following condition is satisfied.

$$e(\sigma_1, \sigma_2, \sigma_3, \sigma_4, gm_6) = e(g_1, g_2)$$

***Proof of Correctness*:**

$$e(\sigma_1, \sigma_2, \sigma_3, \sigma_4, gm_6) = e(c_1 \cdot gm_1 \cdot y^d \cdot gm_2 \cdot y_1^d \cdot gm_7, g_2^{\frac{1}{(m+n)}})$$
$$= e(y \cdot g_1^m \cdot g_1^m \cdot g_1^{xd} \cdot g_1^{-x} \cdot g_1^{-m} \cdot g_1^{-xd} \cdot g_1^n, g_2^{\frac{1}{(m+n)}})$$
$$= e(g_1^x \cdot g_1^m \cdot g_1^m \cdot g_1^{xd} \cdot g_1^{-x} \cdot g_1^{-m} \cdot g_1^{-xd} \cdot g_1^n, g_2^{\frac{1}{(m+n)}})$$
$$= e(g_1^{x+m} \cdot g_1^{-(x+m)} \cdot g_1^{m+n}, g_2^{\frac{1}{(m+n)}})$$
$$= e(g_1^{m+n}, g_2^{\frac{1}{(m+n)}})$$
$$= e(g_1, g_2)^{\frac{m+n}{m+n}}$$
$$= e(g_1, g_2)$$

For message integrity

$$e(\sigma_5, g_2^{RHF}) = e(g_1, g_2)$$

***Proof of Correctness*:**

$$e(\sigma_5, g_2^{RHF}) = e(g_1^{\frac{1}{SHF}}, g_2^{RHF})$$
$$= e(g_1^{\frac{1}{H_1(mes)}}, g_2^{H_1(mes)})$$
$$= e(g_1, g_2)^{\frac{H_1(mes)}{H_1(mes)}}$$
$$= e(g_1, g_2)$$

4.4 Service Provider's Anonymous Authentication

Before providing access to the mobile users, the service providers' needs to check the legitimacy of the mobile users to avoid communication with the illegal users.

$e(gm_3 \cdot gm_4 \cdot gm_5, Y_2) = e(g_1, g_2)$

***Proof of Correctness*:**

$$
\begin{aligned}
& e\left(gm_3 \cdot gm_4 \cdot gm_5, Y_2\right) = e(Y_1^{m+z} \cdot Y_3^{-m} \cdot Y_4^{-m}, g_2^{\frac{1}{(l+s)z}}) \\
& = e(Y_1^m \cdot Y_1^z \cdot Y_3^{-m} \cdot Y_4^{-m}, g_2^{\frac{1}{(l+s)z}}) \\
& = e(g_1^{(l+s)m} \cdot g_1^{(l+s)z} \cdot g_1^{-lm} \cdot g_1^{-ms}, g_2^{\frac{1}{(l+s)z}}) \\
& = e(g_1^{(l+s)m} \cdot g_1^{(l+s)z} \cdot g_1^{-m(l+s)}, g_2^{\frac{1}{(l+s)z}}) \\
& = e(g_1^{(l+s)z}, g_2^{\frac{1}{(l+s)z}}) \\
& = e(g_1, g_2)^{\frac{(l+s)z}{(l+s)z}} \\
& = e(g_1, g_2)
\end{aligned}
$$

If it holds, the SP ensures that the mobile user is a legitimate user, otherwise, the SP avoid communication with the mobile user.

5. SECURITY ANALYSIS

In this section, we briefly analyze our proposed protocol with some security and privacy issues.

5.1 Impersonation Attack

In our proposed schemes, to perform an impersonation attack, the attacker should derive the temporary short time keys owned by a legitimate mobile user and the service provider. Moreover, the attacker should derive the private keys issued by the TP to a particular mobile user. However, the attacker cannot compromise the registration protocol because it is performed in offline mode directly in the TP. Hence, our system is secure against impersonation attack.

5.2 Message Integrity

In general, the message integrity can be ensured by the mobile user through the bilinear pairing process. In the anonymous secure mutual authentication, the message integrity can be achieved using both hash function and the bilinear pairing function that is mentioned as follows $e(\sigma_5, g_2^{RHF})$. If there is any modification in the message transmission, the value of *SHF* will be different from the value of *RHF*. Hence, the message integrity is achieved in this proposed work.

5.3 Anonymity

With the given public keys given by the TP to the mobile user and to the service

provider, it is computationally hard to identify the actual sender of the message. Hence, the attacker gets no knowledge about the sender from the public keys given by the TP.

5.4 Source Authentication

The mutual authentication between the user to service provider and the service provider to the user are performed in an anonymous manner. In this authentication process, each user and each service provider check the legitimacy of the user or service provider using the general parameter $e(g_1, g_2)$. In the case of masquerading, the users and service providers cannot get this general parameter after successful authentication. In order to get this condition, the service provider and the user are required to register their identities in the TP and also it is necessary to get the authentication parameters from the TP.

6. PERFORMANCE ANALYSIS

In this section, we analyze the performance of our anonymous authentication scheme in terms of computational cost with some of the existing schemes. We also compare the performance of the proposed anonymous authentication scheme with four most recently proposed authentication schemes. In our scheme, we use bilinear pairing $G_1 \times G_2 \rightarrow G_3$ to achieve the security where G_1, G_2 and G_3 are the cyclic group generated by a point p with the order q on the elliptic curve $E = y^2 = x^3 + x \bmod q$.

Computational Cost

In this section, we analyze the computation costs of the related anonymous authentication schemes for mobile cloud computing. For convenience, we define some notations about execution time as follows,

T_p–Execution time of a bilinear pairing operation.
T_m–Execution time of a multiplication operation.
T_{add}–Execution time of an additional operation.
T_h–Execution time of a hash function operation.

To compare the computation cost related to the anonymous authentication scheme for VANETs, we compute the execution time of operations using Cygwin platform integrated with the windows operating system. The execution time of different cryptographic operations are shown in Table 2.

Table 2. Execution time of different cryptographic operations.

Cryptographic operation	Execution time (milliseconds)
T_p	0.28
T_m	0.001
T_{add}	0.000
T_h	1.07

The performance analysis of various existing schemes [16-19] are compared with the proposed scheme in Table 3.

Table 3. Comparison of computation cost.

Scheme	Single message verification	n message verification
CPAS [16]	$3T_p+2T_m+T_{add}+2T_h$	$3T_p+(n+1)T_m+3(n-3)T_{add}+2nT_h$
SSBVGT [17]	$3T_p+2T_m+T_{add}+3T_h$	$3T_p+(3n+1)T_m+(3n-2)T_{add}+3(n)T_h$
CAS [18]	$3T_p+T_m+2T_h$	$3T_p+(n)T_m+(3n-3)T_{add}+2nT_h$
EICPAS [19]	$3T_m+2T_h+2T_{add}$	$(3n+2)T_m+(3n-1)T_{add}+2nT_h$
Our proposed scheme	$3T_p+T_h$	$(1+2n)T_p+nT_h$

The comparison of the computational cost for each step is presented in Table 3. For single message verification in CPAS [16], the user needs to execute three pairing operations related to bilinear pairing, two multiplication operations related to bilinear pairing, one addition operation and two hash function operations. Therefore, the execution time of this step is $3T_p+2T_m+T_{add}+2T_h$ = 2.982ms. For multiple message verification the verifier needs to execute three pairing operations, $(n + 1)$ multiplication operations, $(3n - 3)$ addition operations and $2n$ hashing operations. Therefore the execution time of this approach is $3T_p+(n+1)T_m+3(n - 3)T_{add}+2nT_h = 2.144n+0.841$ms.

For single message verification in SSBVGT [19], the user needs to execute three pairing operations and two multiplication operations along with one addition operation and three hash function operations. Therefore the execution time of this scheme is $3T_P+2T_m+T_{add}+3T_h$ = 4.052ms. For multiple message verification, the user needs to execute three pairing operations related to bilinear pairing, $(3n + 1)$ multiplication operations, $(3n - 2)$ addition operations and $3(n)$ hashing operations. Therefore the execution time of this scheme is $3T_p + (3n + 1)T_m + (3n - 2)T_{add} + 3(n)T_h = 3.213n+.0.841$ms. For single message verification in CAS [18], the user needs to execute three pairing operations, one multiplication operation and two hash function operations. Therefore the execution time of this method is $3T_p+T_m+2T_h$ = 2.981ms. For multiple message verification the user needs to execute three pairing operations, (n) multiplication operations, $3(n - 3)$ addition operations and $2n$ hashing operations. Therefore the execution time of this step is $3T_p + (n)T_m+(3n - 3)T_{add} +2nT_h = 2.141n+0.84$ms.

For single message verification in EICPAS [19], the user needs to execute three pairing operations, two addition operations and two hash function operations. Therefore, the execution time of this step is $3T_m+2T_h+2T_{add}$ = 2.143ms. For multiple message verification, the user needs to execute $(3n+2)$ multiplication operations, $(3n - 1)$ addition operations and $2n$ hashing operations. Therefore, the execution time of this method is $(3n + 2)T_m+(3n - 1)T_{add} +2nT_h = 2.143n+.0.002$ms.

In our scheme to verify a single message, the mobile user needs to execute three pairing operations and two hashing function operations. Therefore, the execution time of our proposed scheme is $3T_p+T_h$ = 1.91ms which is very less compared with above schemes. For multiple message verification, our scheme requires only $(1+2n)$ pairing operations and (n) hashing operations. Therefore, the execution time of this proposed scheme is $(1+2n)T_p+nT_h = 1.63n+0.28$ms.

In Fig. 2, the computation time for verifying n number of messages for the previously proposed four schemes is compared with computation time for verifying n number

of messages of proposed scheme. Fig. 2 shows that our proposed scheme shows the less computation time comparing with other existing schemes.

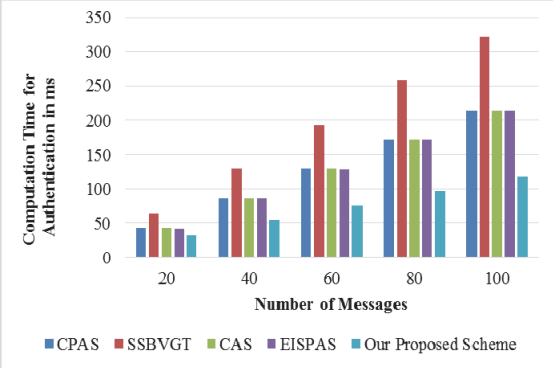

Fig. 2. Execution time for the verification of multiple messages.

7. CONCLUSIONS

In this paper, we have proposed an efficient authentication scheme for mobile cloud computing based on bilinear pairings. The proposed scheme has been developed to support the mutual authentication between the user and the service provider. The proposed scheme has reduced the computational cost during the authentication process. Our scheme also supports user anonymity and to preserve the real identity of the users from other users in the network. The performance analysis has shown that the computation cost for the anonymous authentication process is very low when compared to the previously proposed schemes. The future works of this work is extended to the batch verification and group authentication.

REFERENCES

1. ABI Research Report, "Mobile cloud applications," http://www.abiresearch.com/research/1003385.
2. X. F. Qiu, J. W. Liu, and P. C. Zhao, "Secure cloud computing architecture on mobile Internet," in *Proceedings of the 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce*, 2011, pp. 619-622.
3. W. Itani, A. Kayssi, and A. Chehab, "Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures," in *Proceedings of the 8th IEEE International Conference on Dependable, Autonomic and Secure Computing*, 2009, pp. 711-716.
4. H. Takabi, J. B. D. Joshi, and G. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security Privacy*, Vol. 8, 2010, pp. 24-31.
5. 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, 2008, pp. 2551-2556.

6. L. Chen and C. Kudla, "Identity based authenticated key agreement from pairings," in *Proceedings of IEEE Computer Security Foundations Workshop*, 2003, pp. 219-233.
7. D. Giri and P. D. Srivastava, "An improved remote user authentication scheme with smart cards using bilinear pairings," Cryptology ePrint Archive, 2006, Report 2006/274.
8. X. J. Tian, *et al*., "Analysis and improvement of an authenticated key exchange protocol for sensor networks," *IEEE Communications Letters*, Vol. 9, 2005, pp. 970-972.
9. C. Tang and D. O. Wu, "An efficient mobile authentication scheme for wireless networks," *IEEE Transactions on Wireless Communications*, Vol. 7, 2008, pp. 1408-1416.
10. G. Yang and C. Tan, "Strongly secure certificateless key exchange without pairing," in *Proceedings of the 6th ACM Symposium on Information*, *Computer and Communications Security*, 2011, pp. 71-79.
11. T. Eissa, S. A. Razak, and M. A. Ngadi, "A novel lightweight authentication scheme for mobile ad hoc networks," *Arabian Journal for Science and Engineering*, Vol. 37, 2012, pp. 2179-2192.
12. H. S. Rhee, J. O. Kwon, and D. H. Lee, "A remote user authentication scheme without using smart cards," *Computer Standards and Interfaces*, Vol. 31, 2009, pp. 6-13.
13. M. L. Das, A. Saxena, V. P. Gulati, and D. B. Phatak, "A novel remote user authentication scheme using bilinear pairings," *Computers and Security*, 2006, Vol. 25, pp. 184-189.
14. M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, Vol. 46, 2000, pp. 28-30.
15. J. Z. Lu and J. Zhou, "Preventing delegation-based mobile authentications from man-in-the-middle attacks," *Computer Standards and Interfaces*, Vol. 34, 2012, pp. 314- 326.
16. K. Shim, "CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Transactions on Vehicular Technology*, Vol. 61, 2012, pp. 874-1883.
17. J. Zhang, M. Xu, and L. Liu, "On the security of a secure batch verification with group testing for VANET," *International Journal of Network Security*, Vol. 16, 2014, pp. 355-362.
18. Z. Gong, Y. Long, X. Hong, and K. Chen, "Two certificates aggregate signatures from bilinear maps," in *Proceedings of the 8th ACIS International Conference on Software Engineering*, *Artificial Intelligence*, *Networking and Parallel Distributed Computing*, Vol. 3, 2005, pp. 188-193.
19. Y. J. Choie, E. Jeong, and E. Lee, "Efficient identity based authenticated key agreement protocol from pairings," *Applied Mathematics and Computation*, Vol. 162, 2007, pp. 179-188.
20. P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad-hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 17, 2016, pp. 1015-1028.

21. P. Vijayakumar, S. Bose, and A. Kannan, "Centralized key distribution protocol using the greatest common divisor method," *Computers and Mathematics with Applications*, Vol. 65, 2013, pp. 1360-1368.
22. P. Vijayakumar, S. Bose, A. Kannan, and L. J. Deborah, "Computation and communication efficient key distribution protocol for secure multicast communication," *KSII Transactions on Internet and Information Systems*, Vol. 7, 2013, pp. 878-894.
23. P. Vijayakumar, S. Bose, and A. Kannan, "Rotation based secure multicast key management for batch rekeying operations," *Networking Science*, Vol. 1, 2012, pp. 39-47.
24. P. Vijayakumar, K. Anand, S. Bose, V. Maheswari, R. Kowsalya, and A. Kannan, "Hierarchical key management scheme for securing mobile agents with optimal computation time," *Procedia Engineering*, Vol. 38, 2012, pp. 1432-1443.
25. S. Audithan, T. S. Murunya, and P. Vijayakumar, "Anonymous authentication for secure mobile agent based internet business," *Circuits and Systems*, Vol. 7, 2016, pp. 1421-1429.

Sivaraman Audithan received B.E. degree from A.V.C. College of Engineering Bharathidhasan University, India in 2000, M.E degree from Annamalai University, Chidambaram, India in 2006, and the Ph.D. degree from Annamalai University, Chidambaram in 2011. From 2001 to 2004, he was a Network engineer for R.B. Comtec Pvt. Ltd in Hyderabad, India. From 2006 to 2007 he was a lecturer in Computer Science and Engineering department at SASTRA University, Tamilnadu, India. From 2007 to 2011, he was a Research Fellow in Annamalai University, India. He is presently working as a Principal at P.R. Engineering College. His research interests are in image processing, computer vision, pattern recognition, and remote-sensing data analysis.

Vijayaregunathan Vijayasaro is currently a Ph.D. Research Scholar at the Department of Information and Communication Engineering, PRIST University, Thanjavur. She earned her ME in Embedded System Technologies from Anna University of Technology, Coimbatore. She completed her BE in Electronics and Communication Engineering from Sudharsan Engineering College Pudukkottai. She worked as a Teaching Fellow in Electrical and Electronics Engineering Department of Anna University, College of Engineering, Gunidy, Chennai from 18th July to till 30th November 2014. She was as an Assistant Professor in Electronics and Communication Engineering Department at Sudharsan Engineering College, Pudukkottai from 1st June 2012 to till 31st May 2013. She has published 5 research papers in reputed journals with high impact factor.

Pandi VijayaKumar completed his Ph.D. in Computer Science and Engineering in Anna University Chennai in the year 2013. He Completed Master of Engineering in the field of Computer Science and Engineering in Karunya Institute of Technology affiliated under Anna University Chennai in the year 2005. He completed his Bachelor of Engineering under Madurai Kamarajar University, Madurai in the year 2002. He was working as a Senior Lecturer in All Nations University Ghana, West Africa from 2007 to 2008. He is presently working as a Dean at University College of Engineering Tindivanam which is a Constituent College of Anna University. His main thrust research areas are key management in network security and multicasting in computer networks.

Varadarajan Vijayakumar is a Professor in the School of Computing Science and Engineering at Vellore Institute of Technology Chennai campus. His primary research interests include cloud computing, grid computing, big data and security. He received the BE and ME degree from Madras University and Ph.D. degree from Anna University and MBA degree from Periyar University. He has more than 14 years of experience in teaching and industry. He has more than 20 publications which includes Journals and Conferences. He is also the reviewer for Springer's Journal of Super Computing and many other journals.