Journal of Ambient Intelligence and Humanized Computing
https://doi.org/10.1007/s12652-020-02765-7

ORIGINAL RESEARCH

Cloud based efficient authentication for mobile payments using key distribution method

A. Saranya[1] · R. Naresh[1]

Received: 14 August 2020 / Accepted: 26 November 2020

Abstract
The extensive usage of clever strategies fascinates numerous considerations on the innovation intended for mobile payment method in the background of cloud computing. Though, payment confidence and customer confidentiality still increase serious anxieties to the use of mobile payments. Subsequently, current authentication procedures for mobile payments moreover have high overhead on source inadequate smart scheme. These schemes cannot deliver customer secrecy in mobile payment. To resolve the tasks smartly we have present a cloud based efficient Authentication for mobile payments using key distribution method. Based on the certificate less proxy re signature system, we have designed a different mobile payment procedure which not only attains secrecy; it also achieves the storage complexity by consuming fewer amounts of data. In our proposed method, the efficiency is particularly enhanced by retaining cost of computation in the payment area. Furthermore, by seeing that the payment area the Merchant Server wishes to achieve computation for every payment operation, the impression of batch authentication was implemented to remove the difficulties faced when more number of customers use the Payment area so that Merchant Server can solve the scalability dispute. By our security analysis discussed in this paper, the proposed method is verified to be safe by using the prolonged CDH issues. Furthermore, the performance results displays the proposed method is reasonable and quick for the source inadequate smart mobiles in cloud.

Keywords Privacy · Authentication · Certificate less cryptographic technique · Mobile payments · Cloud

1 Introduction

Through the growth and universality of mobile payment platform was proposed by Qin et al. (2017) and Apple pay smart mobiles are extensively utilized in regular life. This makes way for growing amount of necessities for numerous online facilities. As a vital portion of online facilities, mobile payments likewise acquire huge considerations so that numerous mobile applications for payments are established namely, apple payment (Chen et al. 2019), ali payment (Atzori et al. 2002) and we chat payment (Hu et al. 2006). Currently, no problem about the customer location, the customer may possibly usage these online payment operation uses to purchase numerous items in the online amenities.

Though, the online payment operation is on-going, the communications used to guarantee legitimacy of payment operation frequently comprise of customers secret identity data that is exposed to dealers. Seeing the undependability and voracity of dealers, the dealers can vend possessions that customer will not like to vend customers individual identity toward third party for profitable price. Instead, a merchant need have the capability to confirm the validity and legitimacy of a payment operation communication, accordingly the customer might guarantee the items that are delivered to truthful customer.

Additionally, the authorization on payment operation communication can avoid customers charge that the customer does not purchase the items. To come across these safety desires, numerous procedures for mobile payment operation are recommended by using cryptographic techniques. These procedures attain the greatest significant safe necessities point out above namely, customer secrecy and

✉ R. Naresh
nareshr@srmist.edu.in

A. Saranya
saranya.arnise@gmail.com

[1] Department of Computer Science and Engineering, School of Computing, College of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Chennai, Tamilnadu 603203, India

Published online: 02 January 2021

confidentiality. When a procedure delivers customer secrecy, whichever dealers and challengers cannot relate a payment operation communication to a customer's identity. Confidentiality defines the base of a communication can be distinguished and some third parties cannot fake the customer payment operation communication deprived of being perceived. Along with safety desires, effectiveness desires to be alarmed in a mobile payment operation procedure.

The quick progress of cloud (Xiong and Sun 2017; Camenisch et al. 2007; Katz 2010) unavoidably fluctuations customers' routine lives, therefore online payment operation by means of a diversity of smart mobiles essential to be measured. For illustration, smooth meters might remuneration designed for electrical energy routinely; clever earphones might compensate on behalf of digital melody virtual network when required. An entire electronic gadget comprising extensively used smart mobiles meets the public issue that their computation cost as well as storage cost is restricted. Therefore, once a payment operation procedure is established, the computation plus essential storage cost have to be little for the source reserved gadgets. Conversely, in old-style payment operation procedures, the public key structure exists to dispute certificates intended for public key of the customer.

Mostly, the power of the public key used in this paper is checked by the certificates distributed using the certificate authority. It is simple to understand that the certificate authority produced a more communication as well as storage space during the removal, storing and dispersal of certificates. Subsequently there occurs an inconsistency between certificate authority and smart mobiles which simply have restricted computation and storage cost while using the cloud. Thus strategy of mobile payment operation procedure not only have issues like certificates based on public key it also have issues like little sources high computation, communication cost. More traffic as well as storage cost is nowadays issue.

To resolve these overhead, we proposed a new payment operation pattern for mobiles that attains secrecy, no attacks and resource reliability. In the outer layer, the contributions of this paper given below,

1. We have proposed the mobile user signing stage.
2. We have proposed the certificate authority resigning stage. A mobile payment operation procedure with mobile user secrecy is represented. In specific, Payment Stage is presented as a reliable alternative in support of mobile users to interrelate by means of merchant server strongly. As a result, it is further safe for mobile users since they must not communicate communications to merchants openly. In addition source intake on the mobile user area is minimized since the chief operations are accomplished on Payment operation area. Moreover, the certificate less based public key encryption method as well as proxy re-signature structure are presented to succeed secrecy. Provided the signature intended for every particular payment operation is utilized to remove fake mobile users. Furthermore, the computation costs, communication space in addition to storage costs are satisfactory for source restricted smart mobiles in the environment of cloud.
3. We have proposed the merchant server verification stage. The payment operation area besides merchant server desires to accomplish calculation for every payment transaction; the drawback for lots of mobile users at the Payment area in addition to merchant server must be considerably minimized to resolve the issue based on scalability. It is simple to notice the verification of signature lead computation cost at the Payment operation area in addition to merchant server. Motivated via Gordon et al. (2002), Sureshkumar et al. (2017) and Liao et al. (2017) the impression of batch authentication have been used to quicken the verification of signature like manifold signatures commencing from dissimilar mobile users on discrete communications can be checked rapidly. Furthermore, the sign starting from the identical mobile user can be additionally batched to attain greater effectiveness.
4. We developed procedure and relate it by means of former prevailing mobile payment operation methods. The outcome of evaluation displays our procedure is realistic and effective in the environment of cloud.

This paper is organized as follows. Section 2 presents the related works. In Sect. 3 describes the System Architecture and preliminaries of the proposed Cloud Based Efficient Authentication for Mobile Payments using key distribution method. Section 4 demonstrates the proposed Cloud Based Efficient Authentication for Mobile Payments using key distribution method working phase. Section 5 describes the security analysis. Section 6 represents the evaluation results. Section 7 describes the conclusions and future works.

2 Related works

Al-Riyami and Paterson (2003), permits validating communications or official papers in a method that denial of service is prohibited and this method has been commonly used for safe software dispersal, e business, e administration, and other applications.

Blaze et al. have proposed the re signature method in 1998. By extending this method to the normal digital signature (Huang et al. 2005; Coron 2000) permits a partially reliable substitution to renovate a signature from mobile user to signature, commencing from delegator scheduled on the similar communication by engaging the re encrypting key. Though, the substitution is not capable to sign whichever communication in support of either one mobile user.

Bring out through transformation possessions; resigning has been realistic in abundant uses comprising certificate administration and cluster sign establishment. In the conservative delegation resigning system, the public keys of the mobile user require to be authorized by the certificate authority earlier to the authentication of sign. To reduce the high cost suffered by the certificates issued by the certificate authority, uniqueness alternative resigning have been presented with the public key of the mobile user can be simply computed from the mobile user widely known individual identity.

However, very big disadvantage of identity alternative resigning is named as key escrow wherever the private key of the mobile user is produced by a completely reliable private key producer (Katz 2008). To resolve in cooperation with the certificates administration in addition to key escrow issues, alternative resigning has certainly been considered in the certificateless method which is based on cryptographic technique which is regularly measured as an midway among out dated besides identity public key based cryptographic technique Alipay, WeChatpay (Xiong et al. 2018a, b; Yeh 2017; Boneh and Franklin 2001; Zhang et al. 2006). The first recognized certificateless alternative resigning is two way, like alternation can be achieved from the transformation performed two ways.

Array of real-world tenders stimulate the structure of alternative resigning with single way possessions (Xiong and Qin 2015). To the extent we recognize that, the structure of certificateless single way resigning is still open. Payment operation Procedures Through the promotion of smart mobiles, investigation about safe mobile payment operation grows extensive consideration (Xiong et al. 2018a, b).

Kamijo et al. (2010) have proposed a mobile payment operation procedure which provisions secrecy, confidence, and scalability based on SMS techniques (Qin et al. 2017; Pfleeger and Pfleeger 2002; Diffie and Hellman 1976; Guo et al. 2010). This scheme has exclusive data like the place and the period in place of the payment operation will guarantee the safety of the payment operation, however this scheme simply supports healthy on behalf of direct payment operation. Sureshkumar et al. (2017) proposed a secure mobile payment operation protocol that attains far-off payment operation. This scheme uses the symmetric key processes plus hash functions to understand unnoticeable, connectionless based model. This scheme also uses dual openings to improve the robustness of the entire scheme. Though, this scheme does not offer denial of service, this feature actually essential in far-off payment operation (Bellare et al. 1998; Kamijo et al. 2010; Yang and Lin 2016).

Subsequently, Yang (2016) have presented a different mobile payment operation procedure that offers the features like secrecy and confidentiality. Even though the expenses for payment operation in their procedure are minor, the expenses aimed at certificates which are utilized to confirm the legitimacy and validity of public keys. Which are appropriately long for the source restricted mobiles in the environment of cloud (Blaze et al. 1998; Hu et al. 2006; Xiong 2014; Pointcheval and Stern 2000). The advantages are expressed in the cloud research work (Shao et al. 2011; Al-Riyami and Paterson 2003; Shamir 1984).

Yeh (2017) have proposed confident mobile payment procedures via certificate less cryptography features separately. The procedure proposed thru the Qin et al. (2017) delivers secrecy, confidentiality and free certificate possessions. Yang (2016) have proposed that that the authentication Ateniese and Hohenberger (2005) of Qin et al. (2017) procedure is uncertain that mobile users while using the less reliable cloud service provider to fraud the merchant server. At that time the authors have upgraded Qin et al. procedure to understand safe authentication. Though, mutually Qin et al. (2017) besides Yang (2016) procedures will create numerous self-styled characters to hide the identity of the actual mobile user, therefore a more of storing cost are paid on the source restricted mobile users.

Yeh (2017) have proposed a payment operation procedure using certificate less cryptography features. In Yeh procedure, a robust certificate less sign which does not require whichever certificate to confirm the validity of public key in addition to private key sets is approved to attain safe payment operation. Yeh procedure has achieved boundless development in the mobile payment operation procedure, so that we can use this payment operation procedure at all time and anyplace with full effective in smart mobiles (Vergnaud 2008; Tang et al. 2019; Kumari et al. 2020).

Suchithra et al. (2020) presented a network condition based low rate attack detection approach in multimedia networks which consider the network conditions like traffic, latency, number of routes available and other conditions in finding low rate attack. Baskar et al. (2018) sketch the application of time variant predicate based approach towards low rate attack detection by approximating the traffic in the network.

Baskar et al. (2018) presents a low rate attack detection scheme which consider the region specific traffic features and its impact in identifying the low rate attacks in detail. Baskar et al. (2018) performs low rate attack detection by combining different approximation models which analyzes the payload, traffic, route features.

3 System architecture and preliminaries

Certificate authority: Certificate authority is used for registering facilities designed for mobile user's application. Simultaneously, Certificate authority similarly dispenses scheme parameters and half-done private keys designed for authenticated mobile users to confirm the entire system effective phase.

Customer android application: Every software has need of a payment operation task which is named as mobile user application. Here we have some examples like Ali, Apple pay, We Chat and many applications. The above said application requires to be recorded using the Certificate authority to get the consistent scheme parameters besides partial private key. It likewise creates its individual mobile user secret parameter plus public key. At that moment mobile user application finishes the sign by means of its complete private key, it comprises of half-done private key (Fig. 1).

Payment platform: It is an application presented by a Certificate authority; it likewise desires to record with the Certificate authority to get system parameters also private key. Concurrently, with the intention of safeguarding the mobile user data of the payment operation, Payment Platform would deliver resign facility, such that Payment Platform converts sign of mobile user application into sign of payment platform.

Merchant server: It is the server which delivers the facilities to the mobile users, checks the accuracy of the payment operation data to confirm the amenities which are delivered to the consistent mobile user. Purposes of our payment operation Procedure is to repel the possible extortions in the procedure of payment operation, a safe payment operation must ensure the subsequent necessities. (1) Mobile user privacy: The actual individualities of mobile users should be exposed by any person excluding payment platform. (2) No hacking: every payment operation data will be hacked by somebody, specifically; every single mobile user can confirm the accuracy of the payment data.

- We have used ECC encryption method. There are also some other encryption methods they are, AES: The advanced encryption standard is a symmetric algorithm and considered very secure. In fact, everyone from the US government to software and hardware companies utilizes this algorithm. This method uses a block cipher rather than a bit-by-bit stream cipher. The block lengths are either 128, 192, or 256 bits. Users must share the key in order for others to access the data, which means they must also secure that key to prevent unauthorized access.
- **RSA**: Rivest-Shamir-Adleman is an asymmetric algorithm that uses a public key for encryption and a unique private key for decryption. This method is typically used for sharing data over an insecure network, which can include database encryption. The key size is between 1024 and 2048 bits, which provides higher security but a significantly slower pace than other methods.
- **3DES**: Triple Data Encryption is another block cipher. It utilizes three 56-bit keys to encrypt data three times, resulting in a 168-bit key. This option is fairly secure, but also slower due to the multiple encryptions. While cur-

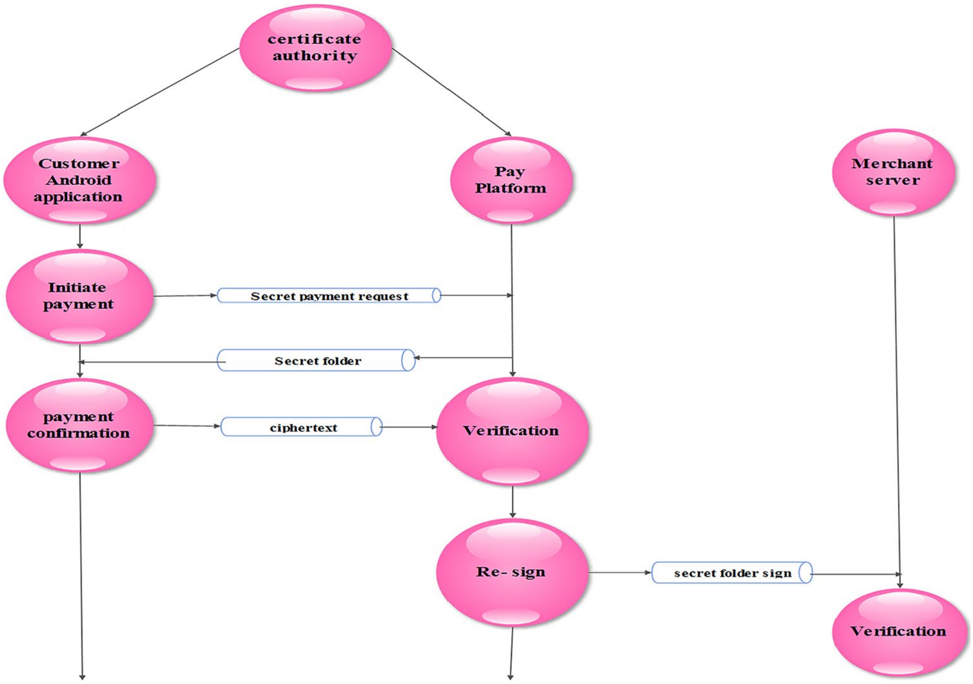

Fig. 1 System architecture of the cloud based efficient authentication for mobile payments using key distribution method

rently in place for a number of businesses, 3DES likely won't last much longer as a standard.

- **Twofish**: Twofish is also a symmetric block cipher, with keys ranging from 128 to 256 bits. It's a fairly flexible method, especially since it's license-free. The number of encryption rounds is always 16, but you can choose whether you want key setup or encryption to be the quicker process.

3.1 Bilinear maps

Now, we practice G1 besides G2 to represent dual cyclic groups through order q. In addition P is a generator of group 1. e: G1 × G1 → G2 is a bilinear mapping, it must gratify the subsequent circumstances:

1. Bilinearity, viz., y,z $\in Z_q$, the equation $e(yp, zp) = e(p, p)$.
2. Non-degeneracy, i.e.,$e(p, p) \neq 1$.

4 Proposed protocols working phase

Setup: Through a safe data l besides a prime digit r, certificate authority produces dual group G1 in addition G2 by order r, and at that point selects a generator q of group1 along with a bilinear pairing $e : G1 \times G1 \rightarrow G2$. Succeeding, certificate authority chooses a confidential key t$\in Z_q^*$ and computes the public key $PK_{PUBLIC} = t.q$. Subsequently, certificate authority selects triple confident hash function h $1 : \{0,1\} * G1 \rightarrow Z_q^*, h2 : \{0,1\} * G1 \rightarrow Z_q^*, h3 : \{0,1\} * \rightarrow G1$. Ultimately certificate authority distributes $G1, G2, e, r, q, PK_{PUBLIC}, h1, h2, h3$ then conserves t confidentially.

How Sha-512 is secure: Sha-512 is very secure, but also takes a lot of database space. If you want to use it, you should still use a salt to improve security. A salt is a string sequence that you add to the user's password to add special characters to it, and makes it longer.

Half private key: Through the parameters, t and mobile user v_i with the mobile user identity $IDEN_i$, certificate authority chooses a indiscriminate number $s_i \in Z_q^*$, and calculates

$$S_i = s_i.q \tag{1}$$

$$I_i = h1\left(IDEN_i, S_i\right) \tag{2}$$

$$t_i = s_i + I_i.tmodr. \tag{3}$$

Subsequently, certificate authority directs the half-done private key,

$E_i = \left(t_i, S_i\right)$ towards v_i and,

v_i checks E_i by testing the following equation

$$t_i \cdot q = S_i + I_i \cdot PK_{PUBLIC}. \tag{4}$$

Moreover,v_i chooses a arbitrary integer $y_i \in Z_q^*$ by means of its confidential key.

Through parameters and y_i, v_i computes $Q_i = y_i.q$ besides arrange Q_i in place of its public based key.

Through the mobile user identity $IDEN_i$ and public key Q_i, along with the mobile user confidential key (E_i ,y_i) related with identity $IDEN_i$ besides public key Q_i, the mobile user calculates

$$re{-}key1_{i,j} = \left(l_i y_i + t_i\right) - 1 \cdot \left(S_i + I_i \cdot PK_{PUBLIC} + l_i Q_i\right) \tag{5}$$

$$re{-}key2_{i,j} = S_i \tag{6}$$

$$key_i = h2\left(IDEN_i, Q_i, S_i, PK_{PUBLIC}\right) \quad \text{and} \tag{7}$$

$$key_j = h2\left(IDEN_i, Q_i, S_i, PK_{PUBLIC}\right) \tag{8}$$

$$re{-}key_{i,j} = re{-}key1_{i,j}, re{-}key2_{i,j}. \tag{9}$$

In conclusion, this procedure yields $re{-}key_{i,j} = re{-}key1_{i,j}, re{-}key2_{i,j}$ as resigning key.

For signing thru parameters, mobile user confidential key (E_i,y_i), mobile user public based key Q_i, individual user identity $IDEN_i$ and communication n, v_i is capable to produce dual types of sign as shown below:

$$\text{Stage 1 :} \quad \alpha_i = \left(\alpha_{1,i}, \alpha_{2,i}\right) = \left(l_i y_i + t_i\right) h3(n), S_i \tag{10}$$

where $key_i = h2\left(IDEN_i, Q_i, S_i, PK_{PUBLIC}\right)$

$$\text{Stage 2 :} \quad \alpha_i = \left[\alpha_{i1}, \alpha_{i2}, \alpha_{i3}, \alpha_{i4}\right], \tag{11}$$

$$\alpha_i = \left(u_i\left(l_i y_i + t_i\right) h3(n), u_i\left(S_i + l_i PK_{PUBLIC} + l_i Q_i\right)\right), u_i.q, S_i \tag{12}$$

where,

$$l_i = h1\left(IDEN_i, S_i\right) \tag{13}$$

$key_i = h2\left(IDEN_i, Q_i, S_i, PK_{PUBLIC}\right)$ and u_i is arbitrarily selected from Z_q^*.

While resigning Through a stage 1 sign $\alpha_i = \left(\alpha_{1,i}, \alpha_{2,i}\right)$ on communication n above the individual identity of the mobile user $IDEN_i$ and mobile user public key Q_i, are sign key $re{-}key_{i,j}$, this procedure is capable to convert the sign α_i to stage 2 sign α_i on the similar communication n based on the individual identity $IDEN_i$ and mobile user public based key (Q_i, S_i) as below.

$$e\left(Q, \alpha_{i1}\right) = e\left(h3(n), \alpha_{i2} + l_i \cdot PK_{PUBLIC} + l_i \cdot Q_i\right). \tag{14}$$

Verifiese$e\left(Q, \alpha_{i1}\right) = e\left(h3(n), \alpha_{i2} + l_i \cdot PK_{PUBLIC} + l_i \cdot Q_i\right)$ is correct or wrong, if this calculation is correct, then it will does the next stages; or else, yields fails.

$$\alpha_i = \left[\alpha_{i1}, \alpha_{i2}, \alpha_{i3}, \alpha_{i4}\right] \tag{15}$$

$$= \left(u_i \cdot \alpha_{i1}, u_i \cdot \left(\alpha_{i2} + I_i \cdot PK_{PUBLIC} + l_i \cdot Q_i\right), u_i.re{-}key1_{i,j}, re{-}key2_{i,j}\right) \tag{16}$$

$$\begin{aligned} &= u_i\left(l_i \cdot y_i + t_i\right)h3(n), u_i\left(S_i + I_i \cdot PK_{PUBLIC} + l_i \cdot Q_i\right), \\ &\quad u_i\left(l_i \cdot y_i + t_i\right) - 1\left(S_i + I_i \cdot PK_{PUBLIC} + l_i \cdot Q_i\right), S_i \end{aligned} \tag{17}$$

$$= u_i\left(l_i \cdot y_i + t_i\right)h3(n), u_i\left(S_i + I_i \cdot PK_{PUBLIC} + l_i \cdot Q_i\right), u_i \cdot QS_i, \tag{18}$$

$$\alpha_i = u_i\left(l_i \cdot y_i + t_i\right)h3(n), u_i\left(S_i + I_i \cdot PK_{PUBLIC} + l_i \cdot Q_i\right), u_i \cdot QS_i. \tag{19}$$

Here u_i is arbitrarily selected from Z_q^* and $u_i = u_i.\left(l_i.y_i + t_i\right)/\left(l_i.y_i + t_i\right)$. It is simple to get α_i is a legal sign at stage 2 on communication n in the individual identity $IDEN_i$ and mobile user public based key Q_i.

Validating thru parameters, a sign α_i on communication n in identity $IDEN_i$ and mobile user public based key Q_i, this procedure is done to confirm the authority of sign: in stage 1: Condition $e\left(Q, \alpha_{i1}\right) = e\left(h3(n), \alpha_{i2} + l_i.PK_{PUBLIC} + l_i.Q_i\right)$ is correct, the sign is success or else, payment operation is fails. In stage 2: Condition $e\left(Q, \alpha_{i1}\right) = e\left(h3(n), \alpha_{i2} + l_i.PK_{PUBLIC} + l_i.Q_i\right)$ besides $e\left(Q, \alpha_{i2}\right) = e\left(\alpha_{i3}, \alpha_{i4} + I_i.PK_{PUBLIC} + l_i.Q_i\right)$ is correct, then the sign is correct or else fails.

5 Security analysis

Chosen plaintext attack: In this technique, the attacker has the manuscript of his excellent encrypted. So the attacker has the cipher text and plain text sets. This makes easy for the attacker job of decisive the encryption based key. An instance of this attack is differential cryptographic technique applied in contradiction of block ciphers in addition to hash functions. A prevalent public key cryptosystem, RSA is also susceptible to chosen plain text attacks.

Brute force attack: In this technique, the attacker attempts to decide the key by trying all probable keys. If the key is 8 bits extended, then the quantity of possible solutions is 256. The attacker distinguishes the cipher text besides the procedure, at this time he tries altogether 256 keys for decryption. The period to finish the attack will be very huge, condition: the key is long.

Man in middle attack: Since we are using the hash function, the attacker cannot attack the mobile user payment operation in the middle. Thus our proposed work will not suffer from the man in the middle attack.

6 Evaluation results

In this evaluvation results part, we calculate the storage time of the Cloud Based Efficient Authentication for Mobile Payments using key distribution method beside many schemes proposed in the survey. The storage time of the Cloud Based Efficient Authentication for Mobile Payments using key distribution method was calculated using language java, Windows 10 (Table 1).

From the Fig. 2: for the protocol 19, the mobile user sign stage requires 21.2 ms, for the certificate authority re-sign stage requires 43.5 ms, for the merchant server verification stage 65.8 ms, and the total storage time took is 98.2 ms. For the protocol 25, the mobile user sign stage requires 10.3 ms, for the certificate authority resigns stage 20.5 ms, for the merchant server verification stage 35.8 ms, the total storage time is 40.2 ms. finally for the proposed, Cloud Based Efficient Authentication for Mobile Payments using key distribution method, for the mobile user sign stage 4.5 ms, for the certificate authority re sign stage 8.6 ms, for the mercant server verification stage 12.6 ms, finally the total storage time for the proposed, Cloud Based Efficient Authentication

Table 1 Notations of the cloud based efficient authentication for mobile payments using key distribution method

S. no	Notations	Descriptions
1	$G1 \times G1 \rightarrow G2$	Cyclic group
2	$e(p, p)$	Bilinear paring
3	S_i	Confidential key of the mobile user
4	s_i, y_i, r	Arbitrary number from the Z_q^*
5	q	Point present in the group
6	$I_i, h1, h2, h3$	Hash function
7	$IDEN_i$	mobile user identity
8	t_i	Randomly computed number
9	PK_{PUBLIC}	Public key of the mobile user
10	$re{-}key1, 2_{i,j}$	Certificate authority resigning key
11	Q_i	Point computed from the cyclic group
12	α_i	Sign of the mobile user

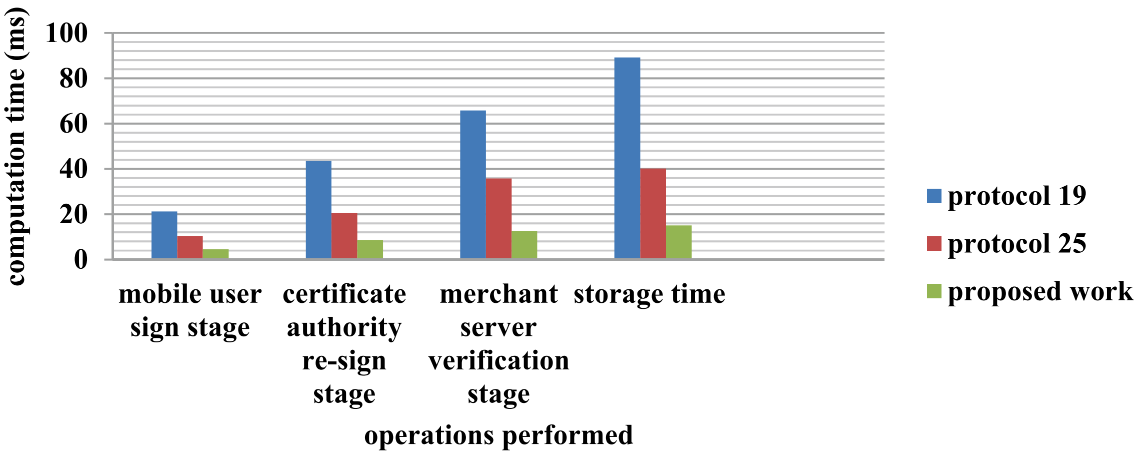

Fig. 2 Storage time for various protocols a

for Mobile Payments using key distribution method is 15 ms. which very less when compared to the other existing procols, thus our proposed work has less storage time when compared to other protocols.

7 Conclusions and future works

In this paper, we have proposed Cloud Based Efficient Authentication for Mobile Payments using key distribution method with the cryptographic system and key distribution technique.The total storage time of the proposed scheme is real-world and mobile user bearable for payment operations.

We have proposed the mobile user sign stage which has low storage time when compared to other protocols, for the protocol 19, the mobile user sign stage requires 21.2 ms, For the protocol 25, the mobile user sign stage requires 10.3 ms, finally for the proposed, cloud based efficient authentication for mobile payments using key distribution method, for the mobile user sign stage 4.5 ms.

We have proposed the certificate authority resign stage which has low storage time when compared to other protocols, for the protocol 19 certificate authority re-sign stage requires 43.5 ms, for the protocol 25, for the certificate authority resigns stage 20.5 ms. for the proposed work for the certificate authority re sign stage 8.6 ms.

We have proposed the merchant server verification stage, which has low storage time when compared to other protocols. for the protocol 19, total storage time took is 98.2 ms, for protocol 25, the total storage time is 40.2 ms, for the proposed protocol, total storage time for the proposed, cloud based efficient authentication for mobile payments using key distribution method is 15 ms.

Moreover, the security power is outstanding level attackers is guaranteed with the subsequent security analysis. From the performance analysis and resulting results, we show that the proposed cloud based efficient authentication for mobile payments using key distribution method is appropriate for smart mobiles. In future, the system performance may be furthermore advanced with the upgrading of the security appliances prefered in the proposed scheme.

References

Al-Riyami SS, Paterson KG (2003) Certificateless public key cryptography. In: Laih CS (ed) Advances in Cryptology - ASIACRYPT 2003. ASIACRYPT 2003. Lecture Notes in Computer Science, vol 2894. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-40061-5_29

Ateniese G, Hohenberger S (2005) Proxyre-signatures: new definitions, algorithms, and applications. In: ACM Conference on Computer and Communications Security, pp 310–319

Atzori L, Iera A, Morabito G (2002) The internet of things: a survey. Comput Netw 54(15):2787–2805

Baskar M, Gnansekaran T (2017) Developing efficient intrusion tracking system using region based traffic impact measure towards the denial of service attack mitigation. J Comput Theor Nanosci 14(7):3576–3582

Baskar M, Gnansekaran T (2017) Multi model network analysis for improved intrusion tracing towards mitigating DDoS attack. Asian J Res Soc Human 7(3):1343–1353

Baskar M, Gnansekaran T, Vijay JF (2018) Time variant predicate based traffic approximation algorithm for efficient low rate DDoS attack detection. TAGA J Graph Technol 14:352–368

Bellare M, Garay J, Rabin T (1998) Batch verification of short signatures. In: International conference on the theory and applications of cryptographic techniques, pp 236–250

Blaze M, Bleumer G, Strauss M (1998) Divertible protocols and atomic proxy cryptography. Lect Notes Comput Sci 1403:127–144

Boneh D, Franklin M (2001) Identity-based encryption from the weil pairing. In: Proc. 21st Annual International Cryptology Conference (CRYPTO 2001), LNCS 2139, pp 213–229

Camenisch J, Hohenberger S, Pedersen M (2007) Batch verification of short signatures. Int Conf Adv Cryptol 4515:246–263

Chen C-M, Xiang B, Liu Y, Wang K-H (2019) A secure authentication protocol for internet of vehicles. IEEE Access. https://doi.org/10.1109/ACCESS.2019.2891105

Coron JS (2000) On the exact security of full domain hash. Advances in cryptology-CRYPTO 2000. LNCS 1880:229–235

Diffie W, Hellman ME (1976) New directions in cryptography. IEEE Trans Inf Theory 22(6):644–654

Gordon S, Kristensen LM, Billington J (2002) Verification of a revised WAP wireless transaction protocol. In: Esparza J, Lakos C (eds) Application and Theory of Petri Nets 2002. ICATPN 2002. Lecture Notes in Computer Science, vol 2360. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48068-4_12

Guo D, Ping W, Dan Y, Yang X (2010) A certificateless proxy resignature scheme. In: IEEE international conference on computer science and information technology, pp 157–161

He D, Kumar N, Khan MK, Wang L, Shen J (2018) Efficient privacy-aware authentication scheme for mobile cloud computing services. IEEE Syst J 12(2):621–1631

Huang X, Susilo W, Mu Y, Zhang F (2005) On the security of certificateless signature schemes from Asiacrypt 2003. In: Proc. Fourth Int'l Conf. Cryptology and Network Security (CANS '05), pp 13–25

Hu BC, Wong DS, Zhang Z, Deng X (2006) Key replacement attack against a generic construction of certificateless signature. In: Proc. 11th Australasian Conference on Information Security and Privacy (ACISP '06), pp 235–246

Kamijo K, Aihara T, Murase M (2010) Anonymity-AwareFace-to-Face Mobile Payment. In: 7th International ICST Conference on Mobile and Ubiquitous Systems: computing, networking, and services (MobiQuitous 2010), LNICST 73, pp 198–209

Katz JE (2008) Hand book of mobile communication studies. The MIT Press, Cambridge

Katz J (2010) Digital signatures. Springer, New York

Kumari A, Kumar V, Abbasi MY, Kumari S, Chaudhary P, Chen CM (2020) CSEF: cloud-based secure and efficient framework for smart medical system using ECC. IEEE Access 8(3):107838–107852

Liao Y, He Y, Li F, Zhou S (2017) Analysis of a mobile payment protocol with outsourced verification in cloud server and the improvement. Comput Stand Interfaces. https://doi.org/10.1016/j.csi.2017.09.008

Pfleeger CP, Pfleeger SK (2002) Security in computing. In: Prentice Hall Professional Technical Reference, pp 182–202

Pointcheval D, Stern J (2000) Security arguments for digital signatures and blind signatures. J Cryptol 13(3):361369

Qin Z, Sun J, Wahaballa A (2017) A secure and privacy-preserving moblie wallet with outsoured verification in cloud computing. Comput Stand Interfaces 54:55–60

Shamir A (1984) Identity-based cryptosystems and signature schemes, vol 21, no 2, pp 47–53

Shao J, Wei G, Ling Y, Xie M (2011) Unidirectional identity-based proxy re-signature. In: IEEE International Conference on Communications, pp 1–5

Suchithra M, Baskar M, Ramkumar J, Kalyanasundaram P, Amutha B (2020) Invariant packet feature with network conditions for efficient low rate attack detection in multimedia networks for improved QoS. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-020-02056-1

Sureshkumar V, Ramalingam A, Rajamanickam N, Amin R (2017) A lightweight two-gateway based payment protocol ensuring accountability and unlinkable anonymity with dynamic identity. Comput Electric Eng 57:223–240

Tang F, Ma S, Xiang Y, Lin C (2019) An efficient authentication scheme for Blockchain-based electronic health records. IEEE Access 7(3):41678–41689

The pairing-based cryptography library (PBC). https://crypto.stanford.edu/pbc/

Vergnaud D (2008) Multi-use unidirectional proxy re-signatures. In: ACM conference on computer and communications security, pp 511–520

Xiong H (2014) Cost-effective scalable and anonymous certificateless remote authentication protocol. IEEE Trans Inf Forensics Secur 9(12):2327–2339

Xiong H, Sun J (2017) Comments on verifiable and exculpable outsourced attribute-based encryption for access control in cloud computing. IEEE Trans Dependable Secure Comput 14(4):461–462

Xiong H, Qin Z (2015) Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. IEEE Trans Inf Forensics Secur 10(7):1442–1455

Xiong H, Mei Q, Zhao Y (2018a) Efficient and provably secure certificateless parallel key-insulated signature without pairing for IIoT environments. IEEE Syst J. https://doi.org/10.1109/JSYST.2018.2890126

Xiong H, Zhang H, Sun J (2018b) Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing. IEEE Syst J. https://doi.org/10.1109/JSYST.2018.2865221

Yang JH, Lin PY (2016) A mobile payment mechanism with anonymity for cloud computing. J Syst Softw 116:69–74

Yeh KH (2017) A secure transaction scheme with certificateless cryptographic primitives for IoT-based mobile payments. IEEE Syst J. https://doi.org/10.1109/JSYST.2017.2668389

Zhang Z, Wong DS, Xu J, Feng D (2006) Certificateless PublicKey signature: security model and efficient construction. In: 4th International Conference on Applied Cryptography and Network Security (ACNS 2006), LNCS 3989, pp 293–308