A Secure Transaction Scheme with Certificateless Cryptographic Primitives Based Mobile Payments

Chaithranjali R S
Department of Computer Science and Engineering,
GSSSIETW,Mysuru

Lakshmi M
Department of Computer Science and Engineering ,
GSSSIETW,Mysuru

Vandana H S
Department of Computer Science and Engineering.
GSSSIETW,Mysuru

Khateeja Ambareen
Department of Computer Science and Engineering.
GSSSIETW,Mysuru

Abstract - How to simultaneously achieve security robustness and maintain the usage convenience of mobile payments within insecure public communication networks is a crucial topic for intelligent mobile device manufacturers, telecommunication companies, and mobile users. In this paper, we introduce a secure transaction scheme with certificateless cryptographic primitives for mobile payments. The proposed scheme takes advantage of the merits of Android Pay and a refined certificate less signature cryptosystem to simultaneously deliver transaction security and achieve payment efficiency in practice. With formally defined adversary model and security analysis, the proposed scheme is proven to be both accurate and secure via random oracle model.It provides strong transaction robustness and communication security to mobile users during online payment transactions. On the other hand, the performance evaluation shows the practicability of our proposed transaction scheme, as the total computation cost is acceptable for a common Internet of Things (IoT)-based test bed.

I. INTRODUCTION

The increasing universality of smart phones, a lot of mobile applications (“apps” for short) have been developed to provide value-added services for mobile users and businesses. In order to support apps running smoothly and effectively, it is crucial to ensure that operating systems are customized for user mobile devices such as smart phones and tablets. Among mobile operating system technologies, Android is one of the most popular platforms, and it has successfully stimulated a generation of numerous Android-based apps all over the world. With more than 80% of the smart phone market share, Android based mobile phone vendors and Internet service providers have to face new challenges related to security and resource management to keep pace with the widespread usage of Android-based mobile apps. The ever-increasing number of mobile services and online transactions involving mobile users’ sensitive personal information heightens the risk of identity theft attacks and other misuses of personal private data. This risk is particularly pronounced whenever mobile users process (or transmit) personal sensitive data by running apps in public network environments without any security protection schemes in place. In addition, new types of online transaction services, such as “in-app purchase” and Considered when designing security solutions for Android-based devices.

In recent years, the payments industry, including mobile device manufacturers, Internet service providers, and telecommunication companies, has evolved to support payments with enhanced protection against counterfeiting, account misuse, and other types of fraud. Famous schemes, such as Apple Pay and Android Pay have been developed with breakthrough contactless payment technology and unique security features built right into the devices that users rely on every day.

In particular, as part of the company’s strategy to acquire and extend its market share, Google Inc., the creator of the Android platform, novel patterns of application services have been developed and deployed in everyday life. Interacting with sensors embedded inside wearable electronics, the interactive operation procedures of the corresponding applications have opened up a whole new range of online application service experiences. Examples of such applications are those related to wellness and fitness, personal health management, healthcare, entertainment, and industrial monitoring. Currently, wearable technology has shown significant potentiality for contactless mobile payments, such as Top shop b Pay accessories and the Fit Pay Smart Strap. Looking forward to the future, it is obvious that contactless mobile payment will likely emerge as the next big thing in terms of wearable consumer devices and wearable technology development. As mobile payment ushers in a new the issue of how to provide transaction robustness for mobile payments under Internet of Things (IoT)-based network architectures will become one of the most important research topics.

The security assurance of the traditional public key infrastructure is based on the certificate, signed by a Certification Authority, containing the relationship between the key pair, i.e., a public key and a private key, and the user’s identity and legitimacy .The issues associated with certificate management, such as revocation, storage, and distribution, will be challenging when facing IoT-based network environments consisting of resource constrained

or bandwidth-limited mobile objects. In contrast to the traditional public key cryptosystem, certificateless cryptography does not require any certificate to ensure the authenticity of public/private key pairs. With this advantage, certificateless public key cryptosystems constitute the possibility for achieving the paradigm of providing robust transaction security for mobile
payments and, at the same time, fulfilling the efficiency requirements of IoT-based intelligent objects. Based on the above discussion, in this paper, we would like to propose a robust transaction scheme adopting an efficient certificateless signature (CLS) crypto-module implemented on Android Pay. First, we extensively survey and investigate the mobile payment mechanisms for Android-based mobile devices and platforms. A refinement of a CLS scheme is then proposed. Furthermore, we integrate the proposed CLS scheme and Android Pay implementation into a new mobile payment scheme. The robustness of the proposed transaction scheme is guaranteed via the formal security analysis and the rigorous performance evaluation we conducted. These results show the feasibility of our proposed scheme and represent our contribution to the development of mobile payment research encourages App developers (or users) to adopt Android Pay as the major payment scheme. Nevertheless, without appropriate protection mechanisms for data transmission, these payment schemes may be insecure against malicious Internet based attacks. Specifically, security properties such as data confidentiality, non repudiation, data integrity, and entity authentication are required to support online transactions (or electronic commerce). Furthermore, the potential threat of user fraud has created a new challenge for mobile payment schemes involving the Android platform, as well as Android device manufacturers, Android App developers, and Android-based device users .Therefore, the design of a robust mobile payment scheme for securing online transactions or electronic commerce is a pressing priority. With the prompt advancement of wearable device technologies

II. PRELIMINARIES

A. Elliptic Curve

Let the notation E/Ep denote an elliptic curve E over a prime finite field Ep , defined by an equation y2 = x3 + ax + b,where a, b ∈ Fp are constants such that Δ = 4a3 + 27b2 _= 0.

All points Pi = (xi, yi) on E and the infinity point O form a cyclic groupGunder the operation of point addition R = P + Q
defined according to a chord-and-tangent rule. In particular, we define t · P = P + P + · · · + P (t times) as scalar multiplication,where P is a generator of G with order n.

Elliptic curve discrete logarithm problem (ECDLP):Given a group G of elliptic curve points with prime order n, a generator P of G, and a point x · P, it is computationally infeasible to derive x, where x ∈ Z∗n .

B. Certificateless Signature

In general, a CLS scheme consists of six phases, i.e., Setup, PartialPrivateKeyExtract, SetSecretValue, SetPublicKey, Sign,and Verify . We briefly review each phase as follows.

1) Setup: With a security parameter k, a trusted third party(TTP), such as a trusted Key Generation Center (KGC) or a Trusted System Authority (TSA), generates a master secret key s, a corresponding master public key PKKGC,and a set of public parameters, i.e., params.

2) PartialPrivateKeyExtract: With the master secret key s,params and the user i's identity IDi , TTP generates apartial secret key Di for the user i.

3) SetSecretValue: The user i randomly selects a value xi ∈Z∗n as his/her secret. With params, the user i's partialprivate keyDi and his/her chosen secret value xi , the user i generates a full private key.

4) SetPublicKey: With params and the user i's secret value xi , the user i outputs his/her public key PKi .

5) Sign: With the message m, this phase outputs a signature σi = (Ri, Ti, τi) on m.

6) Verify: With the signature σi = (Ri, Ti, τi) of the message m, this phase returns 1 if σi = (Ri, Ti, τi) is valid.Otherwise, it returns 0.iversality of wearable consumer electronics.

III. PROPOSED CLS SCHEME FOR MOBILE PAYMENTS

In this section, we propose a new CLS scheme which eliminates the need for the heavy computation of bilinear pairings.

The efficiency of the proposed scheme can thus be guaranteed and it is suitable for mobile communication architecture. Robust security is provided under the hardness of the ECDLP. The proposed CLS mechanism consists of six phases, i.e.,Setup,PartialPrivateKeyExtract, SetSecretValue, SetPublicKey, Sign, and Verify. The details of these six phases are presented as follows.

1) Setup: Given a security parameter k, KGC generates
a group G of elliptic curve points with prime order n and determines a generator P of G. Then, KGC chooses a master key s ∈ Z∗n and a secure hash functionH : {0, 1}∗ × G → Z∗ q . Next,KGCcalculates a master public key PKKGC = s · P. Finally, KGC publishes params = {G, P, PKKGC,H} and keeps s securely.

2) PartialPrivateKeyExtract: Given params, s, and theidentity IDi of user i, KGC generates a random number ri ∈ Z∗ n , and calculates Ri = ri · P, hi = H(IDi ,Ri, PKKGC), and si = ri · IDi hi · s mod n. Then,KGC returns a partial private key Di = (si,Ri) to the user i who checks the validity of Di via whether the equation si · P = Ri · IDi + hi · PKKGC mod n holds or not.

3) SetSecretValue: The user i picks a random number xi ∈Z∗n as his/her own secret value.

4) SetPublicKey: Given params and xi , the user i computes PKi = xi · P as his/her public key.

5) Sign: Given params, Di , xi , and a message m, theuser i generates a signature for m via the followingcomputations.
a) Choose a random number ti ∈ Z∗n .
b) Compute ki = H(m, Ti, PKi , hi), Ti = ti · P andτi = ti + ki · (xi + si) mod n.
c) Output σi = (Ri, Ti, τi) as the signature of the message m.

6) Verify: Given params, IDi , PKi , m, and σi = (Ri, Ti, τi), the verifier examines the validity of σi via the following computations.
a) Compute hi = H(IDi, Ri, PKKGC) and ki = H(m, Ti, PKi , hi).
b) Examine if τi · P = Ti + ki · (PKi + IDi · Ri + hi ·PKKGC) holds. The correctness of the signature σi =(Ri, Ti, τi) is presented as follows:
τi · P = (ti + ki · (xi + si)) · P
= ti · P + ki · (xi + ri · IDi + hi · s) · P
= Ti + ki · (xi · P + ri · IDi · P + hi · s · P)
= Ti + ki · ((xi · P + IDi · Ri) + hi · PKKGC)
= Ti + ki · (PKi + IDi · Ri + hi · PKKGC) .

IV. PROPOSEDTRANSACTION SCHEME FOR ANDROID-BASEDMOBILE PAYMENTS

In this study, we envision the mobile payment environment involving intelligent mobile objects, such as handheld smartphones, fixed/mobile sensors, and wearable devices, which can provide sufficient computation power to perform cryptomodules during the transactions of online payments. The proposed
CLS scheme is integrated into the normal transaction sessions of Android Pay services as a new secure transaction scheme for Android-based mobile payment. In the proposed transaction scheme, we adopt the key agreement operation based on the elliptic curve assumption as the major security component. This design satisfies the intrinsic requirement of not exceeding the resource limitations of Android-based intelligent devices.

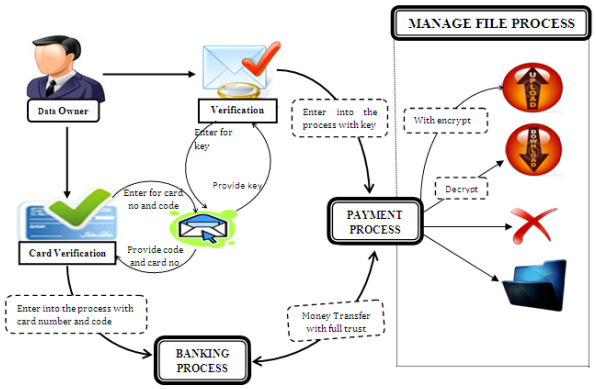
A. System Initialization
Given a security parameter *k*, a TSA generates a group *Go* elliptic curve points with prime order *n* and determines a generator *P* of *G*. Note that the TSA is defined as a trusted security service provided by the Google Play Services or a TTT, such as a cooperating bank supporting the Android Pay service. First, the TSA picks a private key $s \in Z*n$ and a robust one-way hash function, i.e., $H : \{0, 1\}* \times G \rightarrow Z q$. Second, the TSA calculates the master public key *PK*TSA = $s \cdot P$ and publishes *params* = {*G*, *P*, *PK*TSA,*H*}. Meanwhile, the user *i* chooses a random number $xi \in Z*n$ as his/her secret value,
and computes$PKi = xi \cdot P$ as the user *i*'s public key. Third, the Android Pay platform chooses a random number *x*AP ∈ $Z*n$ as its secret value, and computes *PK*AP = *x*AP · *P* as the public key of this platform.

V. ALGORITHM AND TECHNIQUES:

1. Symmetric key algorithm:
Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption.

2.Secret sharing techniques:
Secret sharing techniques refers to method for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number, of possibly different types, of shares are combined together; individual shares are of no use on their own. Secret sharing schemes are ideal for storing information that is highly sensitive and highly important. Examples include: encryption keys, missile launch codes, and numbered bank accounts. Each of these pieces of information must be kept highly confidential, as their exposure could be disastrous; however, it is also critical that they not be lost. Traditional methods for encryption are ill-suited for simultaneously achieving high levels of confidentiality and reliability. This is because when storing the encryption key, one must choose between keeping a single copy of the key in one location for maximum secrecy, and keeping multiple copies of the key in different locations for greater reliability. Increasing reliability of the key by storing multiple copies lowers confidentiality by creating additional attack vectors; there are more opportunities for a copy to fall into the wrong hands. Secret sharing schemes address this problem, and allow arbitrarily high levels of confidentiality and reliability to be achieved.

VI. SYSTEM ARCHITECTURE:



VII. CONCLUSION

In this paper, we have demonstrated a novel transaction process consisting of the implementation of the Android Pay API and the designed CLS cryptosystem. The total computation cost of the proposed scheme is reasonable and user-acceptable for online transactions, in that 2.82 ms at most are required for generating (and examining) each verification message. Furthermore, the security robustness against super-level malicious adversaries is guaranteed with the derived formal analysis. In brief, according to the analysis and evaluation results, we prove that the proposed transaction scheme is practical for common intelligent mobile devices (and mobile networks).

In the future, the system performance may be further improved with the enhancement of the security components adopted in the proposed scheme.

REFERENCES

[1] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security*, 2003, pp. 452–473.

[2] X. Huang, Y. Mu, W. Susilo, D. S. Wong, and W. Wu, "Certificateless signature revisited," in *Proc. 12th Australasian Conf. Inf. Security Privacy*,2007, pp. 308–322.

[3] K.-H. Yeh, "Cryptanalysis ofWang et al's certificateless signature scheme without bilinear pairings," Nat. Dong Hwa Univ., Hualien, Taiwan, Tech. Rep. NDHUIM-IS-2017-001, 2016.

[4] I. Lacmanovi, B. Radulovi, and D. Lacmanovi, "Contactless payment systems based on RFID technology," in *Proc. 33rd Int. Conv. MIPRO*, 2010, pp. 1114–1119.

[5] L. Mainetti, L. Patrono, and R. Vergallo, "IDA-Pay: An innovative micropayment system based on NFC technology for Android mobile devices," in *Proc. 20th Int. Conf. Softw., Telecommun. Comput. Netw.*, 2012, pp. 1–6.

[6] B. Cha and J. W. Kim, "Design of NFC based micro-payment to support MD authentication and privacy for trade safety in NFC applications," in *Proc. 7th Int. Conf. Complex, Intell. Softw. Intensive Syst.*, 2013, pp. 710–713.

[7] E. Kazan and J. Damsgaard, "A framework for analyzing digital payment as a multi-sided platform: A study of three european NFC solutions," in *Proc. Eur. Conf. Inf. Syst.*, 2013, Paper 155.

[8] W.-D. Chen, K. E. Mayes, Y.-H. Lien, and J.-H. Chiu, "NFC mobile payment with citizen digital certificate," in *Proc. 2nd Int. Conf. Next Gener. Inf. Technol.*, 2011, pp. 120–126.

[9] E.-O. Blassa, A. Kurmusb, R. Molvac, and T. Strufed, "PSP: Private and secure payment with RFID," *Comput. Commun.*, vol. 36, no. 4, pp. 468– 480, 2013.

[10] T. Ali and M. A. Awal, "Secure mobile communication in m-payment system using NFC technology," in *Proc. 2012 Int. Conf. Informat., Electron. Vision*, 2012, pp. 133–136.

[11] S. Sung,C. Youn, E. Kong, and J. Ryou, "User authentication using mobile phones for mobile payment," in *Proc. 2015 Int. Conf. Inf. Netw.*, 2015,
pp. 51–56.

[12] R. Magnier-Watanabe, "An institutional perspective of mobile payment adoption: The case of Japan," in *Proc. 47th Hawaii Int. Conf. Syst. Sci.*, 2014, pp. 1043–1052.

[13] S. Abughazalah, K. Markantonakis, and K. Mayes, "Secure mobile payment on NFC-enabled mobile phones formally analysed using casper
FDR," in *Proc. IEEE 13th Int. Conf. Trust, Security Privacy Comput. Commun.*, 2014, pp. 422–431.

[14] B. Ojetund, N. Shibata, J. Gao, and M. Ito, "An endorsement-based mobile payment system for a disaster area," in *Proc. IEEE 29th Int. Conf. Adv. Inf. Netw. Appl.*, 2015, pp. 482–489.

[15] W.-M. To and L. S. L. Lai, "Mobile banking and payment in China," *IT Prof.*, vol. 16, no. 3, pp. 22–27, 2014.

[16] Android Pay API Process Flow, 2016. [Online]. Available: https:// developers.google.com/android-pay/diagrams. Accessed on: Aug. 2, 2016.

[17] Android Pay API Tutorial, 2016. [Online]. Available: https://developers. google.com/android-pay/android/tutorial. Accessed on: Aug. 2, 2016.