An Enhanced Mobile Payment Security Scheme (EMPS) Using ECC Over Binary Field ($F2^m$) and IMEI

[1]T. M. Okediran, [1]O. R. Vincent, [1]A. Abayomi-Alli, [2]O. J. Adeniran
[1]Department of Computer Science, College of Physical Sciences, Federal University of Agriculture, Abeokuta, Ogun state. Nigeria.
[2]Department of Mathematics, College of Physical Sciences, Federal University of Agriculture, Abeokuta, Ogun state. Nigeria.
Email: Vincent.rebecca@gmail.com

Abstract— *The progress of mobile payment research over the last decade till now has been critically assessed, yet security issue still occurring. Existing schemes are not sufficient to combat all the security issues in mobile payment from security of system perspective and usability. Hence, we proposed an enhanced mobile payment security scheme (EMPS) using Elliptic curve cryptography (ECC) over binary field for encryption and International mobile equipment identity (IMEI) for user's identity. Payment details are stored on the payment gateway which can encrypt but cannot decrypt without the merchant's decryption key. It provides integrity, user anonymity, fairness, shorter key size, usability and non-repudiation together with other security features considering mobile phone limitations. It prevents man in middle attack, identity theft, insider attack and others.*

Keywords— **Security, Payment gateway, Cryptography, ECC, IMEI, Mobile payment.**

I. Introduction

Mobile payment is fast growing e-cash transaction in electronic payment, because mobile devices such as smartphones and tablets are quickly becoming the dominant devices for accessing internet resources (Wang *et al.,* 2014; Wang *et al.,* 2016; Antovski & Gusev, 2003; Javidan & Perbonyeh, 2010; Rahmani *et al.,* 2012; Nseir *et al.,* 2013).
In recent times, mobile devices are often shared by multiple applications and used for multiple purposes, which could result in breach of data in financial transactions. Such financial data breach includes illegal access to confidential data, identity fraud, man in the middle attack, malware, phishing, spaming (Wang *et al.,* 2016; Alkhateeb *et al.,* 2015; Chaudhry *et al.,* 2015; Islam *et al.,* 2016), public dispersion of mobile phones (Javidan & Perbonyeh, 2010), risk around privacy and theft (Olanrewaju *et al.,* 2012) and security of user's data with valid credentials is crucial in internet of things (Rafidha & Veni, 2017). Payment information are therefore exposed to compromise. Hence, fraud and identity theft becomes (Rafidha & Veni, 2017; Alkhateeb *et al.,* 2015; Reza & Pirbonyeh, 2010; Mohit *et al.,* 2017).

Several efforts had been devoted to addressing some of these challenges associated with mobile payement fraud and some models has been proposed. It includes biometric authentication (Ahsan *et al.,* 2016); cloud-based payment gateway (Yang & Lin, 2016); anonymous gateway payment protocol (Isaac and Zeadally, 2012); secure wireless payment protocol (Javan & Bafghi, 2014); Rivest Sharmar Addleman (RSA) concept for mobile users (Mohit *et al.,* 2017); Lightweight Payment protocol (Isaac *et al.,* 2012) and Secure Mobile Payment System using QR Code (Nseir *et al.,* 2013).

This work proposed an enhanced mobile payment security scheme (EMPS) using elliptic curve cryptography (ECC) over binary field and international mobile equipment identity (IMEI) with the major contributions as follows: The use of ECC over a binary finite field (**$F2^m$**) on a payment gateway as an encryption protocol provides confidentiality and security means against attacks. The incorporation of mobile phone IMEI to protect against identity theft and non-repudiation. Usability and proper protocol design considering computational power, shorter key size and other limitations. This scheme can be used on a merchant's website and a business to business transaction where both entities are registered party on the payment gateway. The user, merchant, issuer and acquirer can communicate with the payment gateway.
This work is organized as follows: Section two provides the review of related works and overview of elliptic curve cryptography over binary field and its domain parameters. Section three presents the proposed scheme and its architecture with discussion. Section four is the implementation of the work. Finally, section five present the result and conclusion.

II. Related Models to Mobile Payment Security

Previous research had examined mobile payment security in different perspectives using several models. Secure Wireless Payment Protocol (SWPP) manages to provide anonymity and privacy of the customer by using a blindly signed pseudo digital certificate and anonymous bank account to protect the customer's identity (Javan & Bafghi, 2014). It is based on the message flow of SWPP and uses SSL, TLS, and WTLS to cover security requirements such as confidentiality and data integrity during the transaction. The number of SWPP signatures used for non-repudiation has been reduced in the proposed protocol. It manages to keep the customer anonymous to the bank and the merchant during the purchase and the payment, without adding anything to the overheads of the payment process.

RSA concept for mobile users designed a secure and efficient electronic payment system for mobile users. Mobile user can directly communicate with the merchant (Mohit *et al.,* 2017). Although, it has better security performance but, it is only linked to merchant website which is also subject to hacking, malicious file execution, cross site scripting, risk to organization and the flaws of RSA still remains (Vijay *et al.,* 2012; Preetha, & Nithya, 2013). There is no direct communication between the client and payment gateway as well as client and issuer (Vijay *et al.,* 2012; Preetha & Nithya, 2013; Jaiswal *et al.,* 2014; Kaur & Kaur, 2016).

Anonymous gateway payment protocol was used to accomplish confidentiality, anonymity, and integrity with performance evaluation showing its execution time on a mobile phone as 11.68 seconds (Isaac & Zeadally, 2014). However, we also find that the mechanism does not provides the fairness and non-repudiation requirements for the e-transaction. The client can deny the transaction because the payment information cannot be linked directly to the client. Moreover, the mechanism uses the redundant symmetric key between the client and the merchant resulting in key management problem (Yang & Lin, 2016). This redundant key is unnecessary because all messages must be transmitted through the payment gateway.

A cloud-based mobile payment gateway by Yang & Lin, 2016. The work presented a mobile payment mechanism with anonymity for cloud computing. Is observed that Yang *et al.'s* scheme is not suitable for cloud computing as it was claimed by Yang using anonymity for cloud client. Considering the fact that the Payment gateway is in the area of cloud. Because, cloud servers are not considered very secure by putting the Payment gateway in cloud, the security of transaction is becoming more dangerous (Kandukuri & Rakshit, 2009; Krutz & Vines, 2010; Mohit *et al.,* 2017). All entities communicate through the payment gateway for payment related request. Moreover, the client cannot communicate directly with the merchant to process the payment request. In short, the security of Yang et al.'s scheme directly depends on the security of payment gateway (Mohit *et al.,* 2017).

Lightweight Payment protocol (Isaac *et al.,* 2012), designed and implemented a lightweight secure

Payment protocol for those scenarios in vehicular Adhoc networks (VANETs) and other mobile environments using symmetric-key operations which requires low computational power where the Merchant cannot communicate directly with the Acquirer to process the payment request and also present practical performance results that can be achieved with the payment protocol.

Secure Mobile Payment System using QR Code (Nseir *et al.,* 2013). It requires two tokens to verify identity. One is the mobile phone which is placed in the customer's pocket, while the other token is proposed to be a QR code, which will exist in the customer wallet, or simply a PIN number.

III. THE PROPOSED EMPS SCHEME USING ECC OVER BINARY FIELD AND IMEI

This section present the proposed EMPS scheme by using ECC over binary field for encryption due to its simplicity in arithmetic with shorter key size and International mobile equipment identity (IMEI) for integrity and non-repudiation. The IMEI number is used by wireless network operator (GSM network) to identify valid devices over the network and to stop the stolen phone from accessing network, if IMEI number is blacklisted by network operator. The IMEI number of the mobile is unique and used only for identification of the device over the wireless network and subscriber has only semi-permanent relation to the IMEI number (Kumar *et al.,* 2015).

The proposed scheme uses the following elements to establish security:

- Username and password: this is used for every user registration on the payment gateway through the mobile phone to create user account.
- Subscriber Identity Module card: the SIM card number for every individual is unique.
- The phone IMEI (International Mobile Equipment Identity) registered on the payment gateway during user's registration to generate mobile PIN.
- The generated or paired key computed by the ECC algorithm over binary field.
- The mobile PIN generated for login through payment gateway.

PROPOSED EMPS ARCHITECTURE

The architecture of the proposed EMPS scheme using ECC over binary field and IMEI for mobile payment security is represented by figure 1. We input the elliptic curve domain parameters and map it to some points on the elliptic curve. The elliptic curve equation over binary field is used for its computation as implemented on the payment gateway.

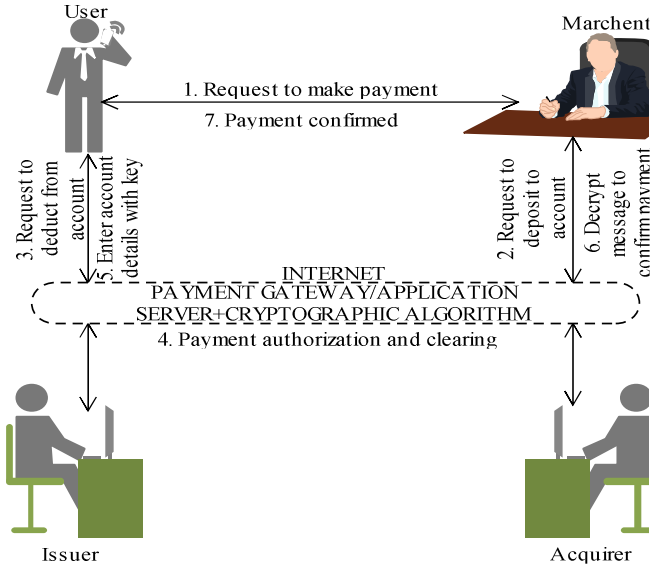

Figure 1: Proposed EMPS Architecture

ENTITIES USED IN THE ARCHITECTURE AND DISCUSSION

The proposed scheme consists of five entities: User (U), Merchant (M), Payment Gateway (PG), Issuer (I) and Acquirer (A).

The user comprises of the SIM and the mobile phone which can initiates a request by dialing a USSD code on the phone or open an application on mobile phone to make payment to the merchant. The first step is to register on the payment gateway to obtain valid credentials needed for transaction. The user is identified by his/her subscriber's identity module (SIM), plus the phone international mobile equipment identity (IMEI) number on a mobile operator network. The login process begins after registration, where the user provides a username and mobile pin to login. A mobile Personal Identification Number (PIN) is generated during user registration using IMEI on the payment gateway and must be available at every login. The merchant receives a request to make payment from the user through the payment gateway. He is also a registered party on the payment gateway. The payment gateway is used in the payment transaction as intermediary between the banks and merchant or User where payment authorization, security and clearing is implemented. An encryption and decryption key is generated through the cryptographic algorithm on the payment gateway using the ECC encryption algorithm over binary field and sent to the user and the merchant respectively. The payment gateway request for the generated key which will be used for encryption on mobile phone and decryption from merchant's end. The issuer is the User's bank who is in the custody of user's money, the acquirer is the merchant's bank who is responsible for receiving money from the issuer on behalf of the merchant.

All entities are registered on payment gateway. Figure 2 shows the transaction sequence.

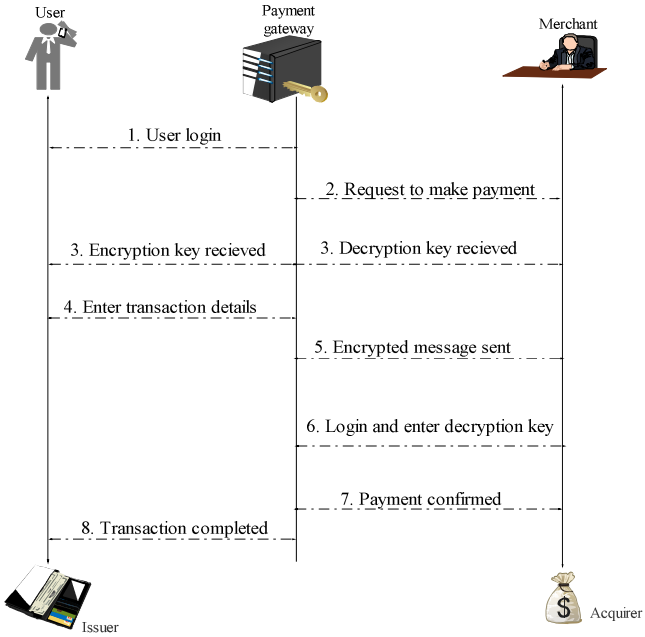

Figure 2: EMPS transaction sequence for mobile payment

THE EMPS PHASES

Registration phase: It is required for user and merchant to register on the payment gateway to obtain valid credentials like mobile pin for login, and to generate encryption key.

Transaction phase: The user send request to make payment to the merchant through the payment gateway and the merchant will have to confirm payment information and details of the user.

Payment authorization phase: This is implemented on the payment gateway through the issuer and the acquirer to validate payment credentials and authorize the payment through the confirmation of the merchant and acquirer and together with the user IMEI registered, key used and issuer's identity.

Payment confirmation: Payment is confirmed from the merchant through the payment gateway to the user, so non-repudiation established.

Key generation and pairing phase: In the key generation phase, an appropriate elliptic curve and the corresponding elliptic curve parameters are chosen to generate the elliptic curve points. The user select private key $n_A \in [1, n-1]$, where n_A key for user and calculate public key $Q_{A=n_AG}$.

The merchant select a private key $n_B \in [1, n-1]$, where n_B key for merchant and calculate public key $Q_{B=n_BG}$.

- Key Exchange: Q_A *and* Q_B
- Shared key computation: $k = n_A Q_B$, $k = n_B Q_A$
  Where $k = n_A Q_B = n_A n_B p = n_B Q_A$.

Algorithm 1: ECC Key Generation Algorithm

Input: Elliptic curve domain parameters over field $F2^m$ (m, f(x), a, b, G, n and h)
Output: Public key Q and private key k
1. Select $k \in_R [1, n-1]$.
2. Compute $Q = kP$.
3. Return (Q, k).

Encryption: The user input plaintext m, the plaintext to be encrypted is converted to binary M. It then calculates the pair of points $C_1 = k * G, C_2 = p + k * Q_B$. That is, $C_1 = kp \; and \; C_2 = M + kp$ using encryption algorithm.

ALGORITHM 2: ECC Mobile Payment Encryption Algorithm

INPUT: plaintext m
OUTPUT: Cipher text C_1, B_2
1. for char $\in m \; do$
2: char$\leftarrow$ *Binary ASCII (char)*
3: char $\leftarrow$ *padding (char)*
4: Append (M, char)
5: end for
6: blocklength $\leftarrow \lfloor N/7 \rfloor$
7: M$\leftarrow$ *Block (M, blocklength)*
8: $k \leftarrow$ *Random* $([1, n-1])$
9: $C_1(x_1, y_1) \leftarrow kP$
10: $C_2(x_2, y_2) \leftarrow M + kQ$
11: for char $\in M \; do$
12: cipher $\leftarrow$ *char* x^2
13: Append $(B_2$*, cipher)*
14: end for
15: return $(C_1(x_1, y_1), B_2)$

Message representation to a point: The ECC cryptosystem deals with the point lying within the defined elliptic curve to perform its operation like key generation, encryption and decryption of text. That is, domain parameters. The plaintext input will be mapped to elliptic curve points during encryption. The point is a randomly generated point on the curve using the ASCII value of the plaintext.

IV. IMPLEMENTATION AND RESULT

The implementation of this work used Java standard edition seven (JavaSe 7) which include a cryptographic engine called SunEC that supports elliptic curve functionality off the shelf. It also support the Java cryptography edition (JavaCE) to manage key agreement, encryption, key generation and manage authentication algorithms (Martinez & Encinas, 2013). The ECC standard used is elliptic curve integrated encryption scheme (ECIES). The Java identifier of the elliptic curve implemented in SunEC provider over binary field as defined in SECG SEC2, ANSI X9.62 and NIST FIPS 186-2 is given in the table below (Martinez & Encinas, 2013).

For the binary field, the element of F_2^m are integers of length m bits and m is a positive integer. The binary equation is an irreducible polynomial of degree $m-1$ and co-efficient can only be 0 or 1. The $f(x)$: $y^2 + xy = x^3 + ax^2 + b$ where x and y are variables chosen from the curve as co-ordinate of any point, *a* and *b* are constant. The number of points chosen to secure the cryptosystem is large and represented with $\#E$ $(F2^m)$, G is the point generator used for successive addition and point doubling during key pairing. Finally, the scalar for point multiplication is chosen as a number between 0 and $n-1$, for n is the range of finite field. The Elliptic curve cryptography deals with the point lying within the defined elliptic curve to perform operation. The plain text input will be mapped to elliptic curve point during encryption. The point is randomly generated on the curve using the ASCII value of the plain text. The major benefit of ECC over binary field is the bit fiddling operation and simplicity in arithmetic, while prime field requires more logic gates.

The proposed scheme is implemented on an Intel core 2 duo CPU speed 2.1 GHz, 4 GB Ram, 32bit windows 7 operating system and 250 GB hard disk.

Registration phase

1. The user open a mobile payment application or dial a USSD code from the mobile phone.
2. The registration requires a user identity (U_{id}) and password to generate a mobile personal identity number (PIN).
3. User enter the login parameters and generate encryption and decryption key needed for secured transaction.
4. The payment gateway performs the key pairing process and send to user and merchant respectively.

Transaction phase

The user is now connected to the issuing bank, the merchant and acquiring bank. At this point the user select the transaction type from the pop-up menus which will include:

a. Change PIN
b. Change registration parameters
c. Request to make payment
d. Register another account
e. Delete account

The user select request to make payment and enter transaction details on the payment gateway. Table 2 is a comparison between other key sizes and the proposed scheme.

TABLE 2: TIME COMPARISON BETWEEN EMPS AND ECC OVER PRIME FIELD.

Key Length in Bit	***Time to generate key***	***Time to generate key for EMPS***	***Encryption time***	***Encryption time for EMPS***	***Decryption time***	***Decryption time for EMPS***	*Time to generate PIN for EMPS*
128	2.15 ms	2.1ms	2.41ms	2.40ms	1.23ms	1.20ms	0.90ms
163	2.33 ms	2.21 ms	2.65ms	2.58ms	1.31ms	1.34ms	1.28ms
192	2.60 ms	2.62 ms	3.18ms	3.10ms	1.57ms	1.47ms	1.52ms

256	2.93 ms	2.86 ms	4.24m s	3.98m s	2.09m s	2.10m s	1.83m s

TABLE 3: SECURITY COMPARISON BETWEEN EMPS AND OTHER SCHEMES

SCHEME	*Isaac& Zeadally*	*Yang & Lin*	*Mohit et al*	*EMPS*
Confidentiality	Yes	Yes	Yes	Yes
Integrity	Yes	Yes	Yes	Yes
Non-Repudiation	No	Yes	Yes	Yes
Anonymity	No	Yes	Yes	Yes
Replay Attack	Yes	Yes	Yes	Yes
Insider Attack	Yes	Yes	Yes	Yes
Impersonation Attack	No	No	Yes	Yes
Identity fraud	No	No	No	Yes
Stolen device recovery	No	No	No	Yes
Shoulder surfing	No	No	No	Yes

Table 3 is the security comparison between reviewed literatures in section two, showing security strength of one scheme against another and compared with the proposed EMPS scheme. Yes indicate agreement that it can combat such attack while No is rejection.

V. CONCLUSSIONS

Mobile payment has improved e-commerce, making life convenient for mobile users. However, security of transactions must be ensured. This paper focused on mobile payment transaction and users' security during transaction over the internet. The use of IMEI provides integrity, non-repudiation and protection against identity theft. While, ECC over binary field used for key generation, encryption and decryption ensures authenticity. The payment detail is protected and stored on the payment gateway to achieve confidentiality and anonymity. This scheme protect users against other known attacks

REFRENCES

[1] Ahamad, S. S., Al-Shourbaji, I., & Al-Janabi, S. (2016). A secure NFC mobile payment protocol based on biometrics with formal verification. *International Journal of Internet Technology and Secured Transactions*, *6*(2), 103-132.

[2] Ahsan, Iqbal, Hussain, & Nadeem (2016). A Mobile Payment Model Using Biometric Technology. International Journal of Advances in Science Engineering and Technology, Vol. 4, Issue-4.

[3] Antovski, L., & Gusev, M. (2003). M-payments. In *Information Technology Interfaces,*

[4] *2003. ITI 2003. Proceedings of the 25th International Conference on* (pp. 95-100). IEEE.

[5] Anoop, M. S. (2007). Elliptic curve cryptography. *An Implementation Guide*.

[6] Boku, "We Care About Payments." [Online]. Available: http://www.boku.com/about/.

[7] Chaudhry, S. A., Farash, M. S., Naqvi, H., & Sher, M. (2016). A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography. *Electronic Commerce Research*, *16*(1), 113-139

[8] Darrel Hankerson, Alfred Menezes & Scott Vanstone. (2004). Guide to Elliptic Curve Cryptography. Springer online.com

[9] Hankerson, D., Hernandez, J. L., & Menezes, A. (2000, August). Software implementation of elliptic curve cryptography over binary fields. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 1-24). Springer, Berlin, Heidelberg.

[10] Dahlberg, T., Guo, J., & Ondrus, J. (2015). A critical review of mobile payment research. *Electronic Commerce Research and Applications*, *14*(5), 265-284.

[11] Ehab M. Alkhateeb, Mohammad A. Alia and Adnan A. Hnaif. (2015). The Generalized Secured Mobile Payment System Based on ECIES and ECDSA, ICIT 2015 the 7th International Conference on Information Technology

[12] Isaac, J. T., & Zeadally, S. (2012). An anonymous secure payment protocol in a payment gateway centric model. *Procedia Computer Science*, *10*, 758-765.

[13] Isaac, J. T., & Zeadally, S. (2014). Design, implementation, and performance analysis of a secure payment protocol in a payment gateway centric model. *Computing*, *96*(7), 587-611. Springer.

[14] Islam, S. H., Amin, R., Biswas, G. P., Obaidat, M. S., & Khan, M. K. (2016). Provably Secure Pairing-Free Identity-Based Partially Blind Signature Scheme and Its Application in Online E-cash System. *Arabian Journal for Science and Engineering*, *41*(8), 3163-3176. Springer.

[15] Isaac, J. T., Zeadally, S., & Cámara, J. S. (2012). A lightweight secure mobile payment protocol

[16] for vehicular ad-hoc networks (VANETs). *Electronic Commerce Research*, *12*(1), 97-123.

[17] Javan, S. L., & Bafghi, A. G. (2014). An anonymous mobile payment protocol based on SWPP. *Electronic Commerce Research*, *14*(4), 635.

[18] Jaiswal, A., Raj, G., & Singh, D. (2014). Security Testing of Web Applications: Issues and Challenges. *International Journal of Computer Applications*, *88*(3). New York.

[19] Javidan, R., & Pirbonyeh, M. A. (2010, November). A new security algorithm for electronic payment via mobile phones. In *Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on* (pp. 1-5). IEEE.

[20] Kaur, D., & Kaur, P. (2016). Empirical analysis of web attacks. *Procedia Computer Science*, *78*, 298-306.

[21] Koblitz, N., Menezes, A., & Vanstone, S. (2000). The state of elliptic curve cryptography. In *Towards a quarter-century of public key cryptography* (103-123).

[22] Kandukuri, B. R., & Rakshit, A. (2009, September). Cloud security issues. In *Services Computing, 2009. SCC'09. IEEE International Conference on* (517-520).

[23] Kumar, K., Kaur, P., & GNDU, A. (2015). Vulnerability detection of international mobile equipment identity number of smartphone and automated reporting of changed IMEI number. *International Journal of Computer Science and Mobile Computing*, *4*(5), 527-533.

[24] Krutz, R. L., & Vines, R. D. (2010). *Cloud security: A comprehensive guide to secure cloud computing*. Wiley Publishing.

[25] Kungpisdan, S., Srinivasan, B., & Le, P. D. (2004, April). A secure account-based mobile payment protocol. In *Information Technology: Coding and Computing, 2004. Proceedings of International Conference on ITCC*, 1, (35-39)

[26] Kavitha, K. (2014). Study on Cloud Computing Model and its Benefits, Challenges. *International Journal of Innovative Research in Computer and Communication Engineering*, *2*(1), 2423-2431.

[27] Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.

[28] Martinez, V. G., & Encinas, L. H. (2013). Implementing ECC with Java Standard Edition 7. *International Journal of Computer Science and Artificial Intelligence*, *3*(4), 134.

[29] Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. *Journal of Network and Computer Applications*, *36*(1), 42-57.

[30] Mohit, P., Amin, R., & Biswas, G. P. (2017). Design of Secure and Efficient Electronic Payment System for Mobile Users. In *International Conference on Mathematics and Computing* (pp. 34-43). Springer, Singapore.

[31] Nseir, S., Hirzallah, N., & Aqel, M. (2013). A secure mobile payment system using QR code. In

[32] *Computer Science and Information Technology (CSIT), 2013 5th International Conference on* (pp. 111-114). IEEE.

[33] Olanrewaju, T., Zavarsky, P., Ruhl, R., & Lindskog, D (2012). Security Modeling of Mobile Payment System Architecture. Journal of Computer Applications. Volume 58, no. 16.

[34] Preetha, M., & Nithya, M. (2013). A study and Performance Analysis of RSA Algorithm. *IJCSMC*, *2*, 126-139.

[35] Rafidha & Veni, S. (2017). Compression and Encryption approach for Data Security in Mobile Internet of Things. *complexity*, *7*, 8. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 6, Issue 1.

[36] Ratnakanth, B., & Avadhani, P. S. (2017). A Review of Secure Authentication based e-Payment Protocol. *International Journal of Advanced Computer Science and Applications*, *8*(3), 150-158.

[37] Rahmani, Z., Tahvildari, A., Honarmand, H., Yousefi, H., & Daghighi, M. S. (2012).Mobile

[38] Banking and its Benefits. *Oman Chapter of Arabian Journal of Business and Management Review*, *2*(5), 38-41.

[39] SET Secure Electronic Transaction Specification, Book 3: Formal Protocol Definition. SET Secure Electron Trans LLC; 1997.

[40] Sutter, G. D., Deschamps, J. P., & Imaña, J. L. (2013). Efficient elliptic curve point multiplication using digit-serial binary field operations. *IEEE Transactions on Industrial Electronics*, *60*(1), 217-225.

[41] Shetty, M. N., Puranik, T., Ghosalkar, S., & Jaybhaye, S. (2014, July). Analysis of Elliptic Curve Cryptography for Mobile Banking. In *International Journal of Engineering Research and Technology* (Vol. 3, No. 7 (July-2014)). IJERT

[42] Suma, A. P., Shankar, S., & Puttamadappa, C. (2016). Secure Transmission of Data In Smart Grid With The Aid Of Elliptic Curve Cryptography Method. *Technology*, *7*(1), 50-63.

[43] Susantio, D. R., & Muchtadi-Alamsyah, I. (2016, April). Implementation of Elliptic Curve Cryptography in Binary Field. In *Journal of Physics: Conference Series* (Vol. 710, No. 1, p. 012022). IOP Publishing.

[44] Sureshkumar, V., Anitha, R., Rajamanickam, N., & Amin, R. (2017). A lightweight two-gateway based payment protocol ensuring accountability and unlinkable anonymity with dynamic identity. *Computers & Electrical Engineering*, *57*, 223-240.

[45] Sultan, N. (2010). Cloud computing for education: A new dawn. *International Journal of Information Management*, *30*(2), 109-116.

[46] Vijay, A., Madhur & Trikha. P. K. (2012). A New Variant of RSA Digital Signature. *International Journal of Advanced Research in Computer Science and Software Engineering*, *2*(10).

[47] Wang, Y., Hahn, C., & Sutrave, K. (2016, February). Mobile payment security, threats, and challenges. In *Mobile and Secure Services (MobiSecServ), 2016 Second International Conference on* (pp. 1-5).

[48] Wang, Y., Vangury, K., & Nikolai, J. (2014, May). Mobile Guardian: A security policy enforcement framework for mobile devices. In *Collaboration Technologies and Systems (CTS), 2014 International Conference on* (pp. 197-202).

[49] Yang, J. H., & Lin, P. Y. (2016). A mobile payment mechanism with anonymity for cloud computing. *Journal of Systems and Software*, Elsivier, *116*, 69-74.

[50] Y. Wang, K. Streff, and S. Raman (2012), "Smartphone Security Challenges," Computer (Long. Beach. Calif). vol. 45, no. 12, pp. 52–58, Dec. 2012.