Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 6 – No.6, January 2017 – www.caeaccess.org

Secured Payment Protocol

Swapna Khandekar
Department of Electrical Engineering and Computer Science
Cleveland State University, Cleveland, OH

Richard Kolk
Department of Electrical Engineering and Computer Science
Cleveland State University, Cleveland, OH

Jingyuan Liang
Department of Electrical Engineering and Computer Science
Cleveland State University, Cleveland, OH

ABSTRACT

In recent years, there is tremendous increase in usage of online payment applications. It is simple, quick and efficient mode of money transfer. From common man to business man, everyone is taking advantage of these applications to make transactions easy. However, with advancements in technology, security threats have increased drastically. In this research paper, secured payment protocol using self- certified key generation method has been suggested.

In order to understand, potential security threats in any payment protocol, one should have clear idea about possible vulnerabilities in it. Considering these vulnerabilities, authors have suggested preliminary version for new payment protocol. In this analysis, authors have used various methodologies like reverse engineering, study of security attacks. Also authors have proposed an energy-efficient model to improve energy efficiency for payment application.This study will be helpful in improving security in payment application and in growth of e – commerce bussiness.

General Terms

Cryptography, Payment Gateway, Encryption, Power Consumption, Mobile Payment app,

Keywords

Key Generation, Social engineering attacks, Energy efficiency, Scalability, Security, Payment Protocol, Private Key, Public Key

1. INTRODUCTION

In today’s world of internet, everything is available on fingertips. One can do shopping, banking, investments, buying or selling sitting at home. These things became possible due to online payment facility [1]. Nowadays, huge payments are done online. No need to worry about carrying large money with yourself. Enhanced security in internet helped users making these secured transactions [2]. Increased use of smart phone is also added advantage in payment procedure. Many payment applications are available suitable for mobile platforms. It seems to be more secure than carrying cash in hand [3].

Money transfer using smartphone is as simple as giving cash from wallet. As there is serious concern of cash thievery with physical cash, similarly, there are security concerns during online money transfer. However, available authentication and authorization method helps to reduce these problems [4]. These methods are also available during online transaction using mobile phones. However, these smartphones have their own attributes like non-transparent use of smartphone devices, features introduced with near-field communication (NFC) and quick response (QR) code etc [5]. As payment using cellphones is comparatively new method of money transfer, hence few security concerns are still not answered [1].

Traditional security issues in web based payment applications are present in mobile based payment application [6]. Also mobile application has their own vulnerabilities which is more challenging for protocol developers. This study mainly focus on mobile based payment applications and security concerns related to it. As very few research paper were found concentrating on smartphone application. Though fundamental concept is not novel [4], however advantages in computer system could be potential flaws for smartphone platform. There could be issues with security related to front end of application (user interface) as well as back end of the application [7]. Payment procedure involves many entities which could harm safety level. Not only that, social engineering attack is serious hazard for ongoing transaction [8].

In online payment applications, people can send money to anyone using their own smartphone devices. Users need to have personal account associated with payment application. It can be created using email id and phone number. For payment procedure, users have to link their debit/ credit card details with this account [9]. Now the best part is, while transferring money to your friends, user doesn’t need to remember those difficult bank details, just using simple details like email id or phone number, one can send money. It seems to be very handy, but these details can be known to anyone which can lead to some fraudulent situation [10].

In rest of the paper, Section 2 talks about problem identification and significance. Section 3 reviews some other related work. Section 4 provides payment protocol. Section 5 gives possible suggestions and finally section 6 and 7 gives advantages and conclusion respectively.

2. PROBLEM IDENTIFICATION AND SIGNIFICANCE

During research survey, few payment applications were closely studied to understand potential vulnerabilities. Also available literature talks about few serious security issues. For example, improper local sensitive data processing and storage, way of handling user input. As mentioned earlier, payment procedure consists of many entities which are distance apart from each other. Communication between them can be misleading due to insufficient transport-layer protection, poor or missing authorization and authentication and weak server-side control [10]. In this research, authors have tried to provide solutions to few those problems [5].

E-commerce is integral part of business operation and individual person’s life. Eventually, security of network handling those transactions has become important aspect for growth of online banking world [1]. This research will be helpful for preventing unauthorized transaction, online theft/ frauds. It can assist in enhancing network privacy, security, integrity and authenticity.

3. RELATED WORK

3.1. Security Research of a Social Payment App and Suggested Improvement

In this research paper, they have done security analysis for one of the social payment application called square cash on based various factors. As per their observations, Square Cash was secured and reliable application for customers to use. Also to enhance security, they have also introduced new payment protocol. Using this protocol, user can send or receive money without any involvement of third party for key generation which reduces various types of security threats [11].

3.2. Security research of social payment app- VENMO

Another application named Venmo is used for security research. They searched for potential technical and social weaknesses in respective application and found few minor issues in that application. They gave some suggestions for Venmo team for application improvement [9]. For the security identified problems, they have proposed their own solutions, like increasing the length and setting rate limits for the authorization, complying with security policies throughout the whole system and keeping secret values (passwords) safely. In this, they have downloaded APK file of android version of VENMO. Compiled version of this file is used understand working this application.

3.3. Security concerns in mobile based applications

Author [3] has described few security concerns which includes denial of service, unauthorized access, theft and fraud. Spamming and viruses can cause denial of service attack. Due to unauthorized access to system, application and data security threats have increased a lot. Researchers have suggested few security tools to deal with theft and fraud issues like encryption ciphers, firewalls, biometrics passwords, public key infrastructure, digital signatures [3], [10].

Few people did study on security attacks for Mobile Ad hoc networks. Leaking secret information, impersonation, and message contamination can happen due to these security attacks. So they proposed routing protocol Cryptographic Hybrid Key Management for MANET. It helped to maintain and improve confidentiality, availability, integrity, authenticity and non-repudiation [11].

4. PAYMENT PROTOCOL

Proposed payment protocol model is based on Self Certified Key Generation, in which they have considered following entities playing crucial role [11][14] as shown in figure 1.

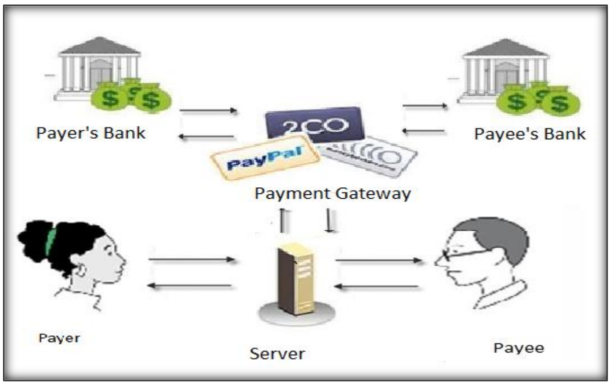


Fig 1 : Operational model for proposed protocol

Payer:
A payer is the one who wish to transfer money to payee. In proposed protocol, the payer is an entity equipped with an Application Unit. In this case Application Unit is Mobile phone in which application is installed.

Server:
Server is an entity to whom payer will contact to make fund transfer. This entity could be a computational one such as a normal web server.

Payee:
A payee is the one who will receive money from payer. The payee is also equipped with an Application Unit. Here, Application Unit is Mobile phone in which application is installed. Here, payee and server is considered as one unit.

Acquirer:
It is payee’s financial institution. It verifies the validity of the deposited payment instrument and manages fund transfer from payee’s end.

Issuer:
It is the payer’s financial institution. It provides electronic payment instruments to the client to use in a payment and manages fund transfer on payer’s end.

Payment gateway:
It is an additional entity that acts as a medium between acquirer/issuer at banking private network side

4.1. Self-certified key

A self-certified key generation protocol provides advantages of certificate-based and identity-based public key cryptosystems. As per Diffie–Hellman assumption, Internal mechanism in user’s end device generates a non-singular elliptic curve E defined over a finite field Fq of characteristic p such a that Fq is used with base point generator P of prime order n. It chooses a key pair (S,Pk), where **Pk = SP**. The related parameter P is public while S is kept secret [11] [13].

4.2 Private key generation

Payer chooses a random number N1 and computes ID such that

N= H1 (ID, N1) P (1)

ID, N1 are send to SA over secure channel.

Payee chooses a random number after receiving this message called N2 and calculates R as a witness payer.

$$\mathbf{R = N + N2P} \tag{2}$$

It computes partial private key X as follows

$$\mathbf{X = H2\ (ID,R)S + N2} \tag{3}$$

Finally Server returns R,X to user over secure channel using which Secret Key Sk can
be calculated

$$\underline{\mathbf{Sk = X + H1(ID,N1)}} \tag{4}$$

4.3 Public key extraction

$Sk = X + H1(ID,N1)$
Considered equation number (4)

$SkP = XP + H1(ID,N1)P$
Multiplied by P both sides

$SkP = H2(ID,R)SP + N2P + H1(ID,N1)P$
As per equation number (3), put value of X

$SkP = H2(ID, R)SP + N2P +N$
As per equation number (1), N= H1(ID,N1)P

$SkP = H2(ID, R)SP + R$
As per equation number (2), N+ N2P = R

$SkP = H2(ID, R)\ Pk + R$
As Pk = SP

$$\underline{\mathbf{Pk\ = (SkP - R\ )/\ H2\ (ID,\ R)}}$$

So user can compute the corresponding public key using above Equation, once they receive the value of witness R and Private key Sk. Refer Table 1 containing notations used in proposed protocol.

Table 1 : Notations used in proposed protocol

Notation	**Description**
ID	Identity of payer
Pk	public key
R	Witness
Sk	Private key
X	Partial private key
Hi(,)	One-way hash function
N1	Random number entered by payer
N2	Random number entered by payee

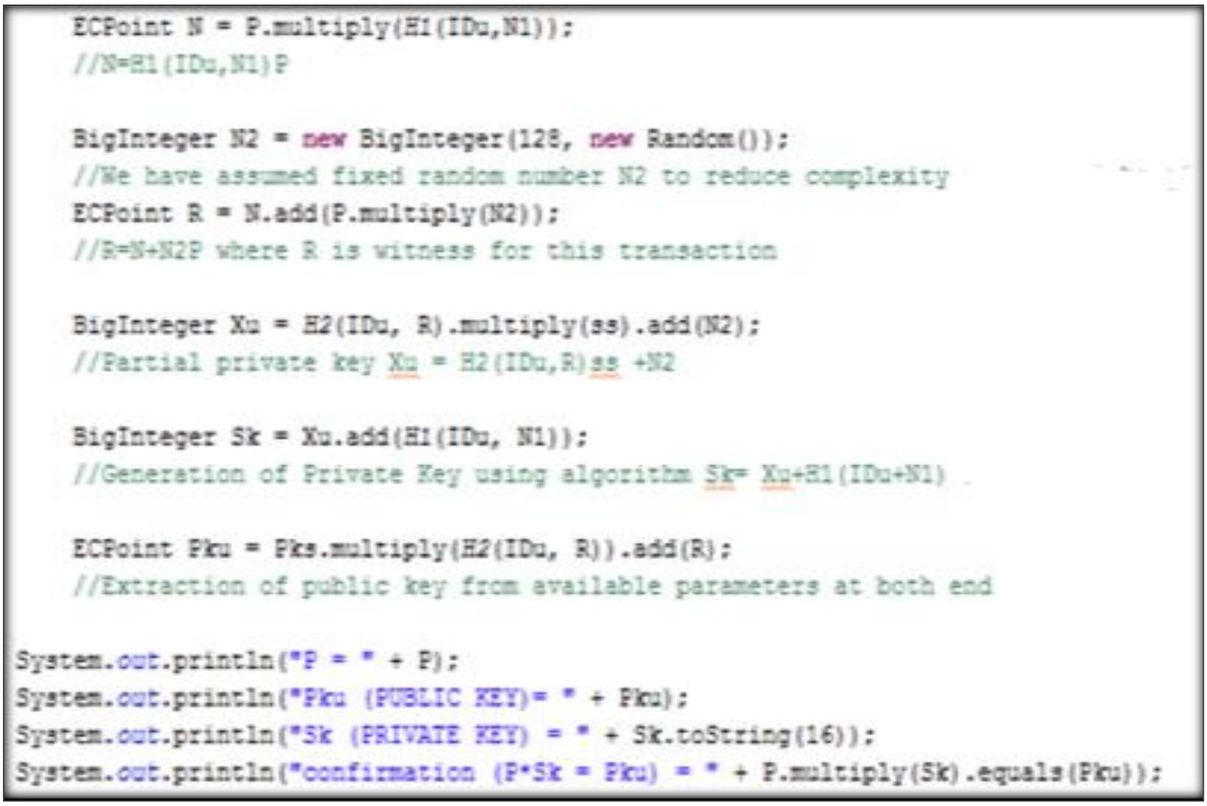
4.4 Flow of payment protocol and implementation

Messages are sent along with keys from payer to payee and vice versa. As mentioned earlier, these key are generated by self certificate agreement protocol. Prior to every transaction these keys are refreshed once to maintain security [11][13].

As shown in Algorithm, payer requests server for authentication. Server also checks payee's details. If payer and payer has valid information, server provides authentication. Payer initiates transactions with new set of keys. Payment gateway verifies, if issuer ban has enough fund or not. Only after confirmation of funds availability, actual transaction takes place. [11]

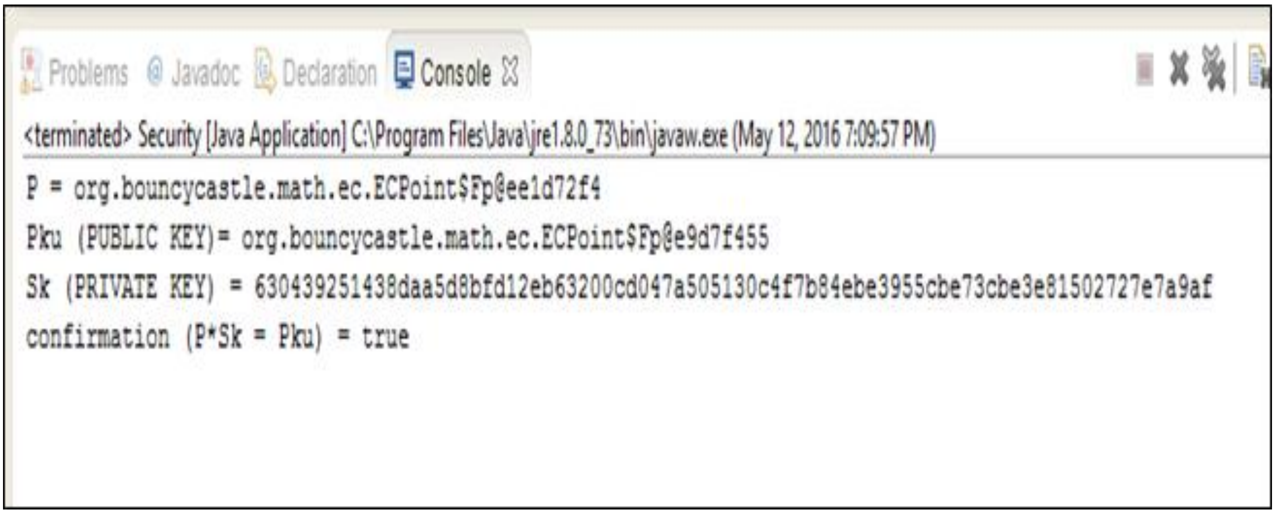
Algorithm

- Start
- Authenticating payer/ payee to server
- If (Payer/Payee credentials =Valid details)
- Initiate Authentication process
- Identification of Private & Public key
- Connect server to payment gateway
- If (Current Balance >=Required Balance)
- Acknowledgement to server
- Acknowledgement to Payer
- Else cancel transaction



```
    ECPoint N = P.multiply(H1(IDu,N1));
    //N=H1(IDu,N1)P

    BigInteger N2 = new BigInteger(128, new Random());
    //We have assumed fixed random number N2 to reduce complexity
    ECPoint R = N.add(P.multiply(N2));
    //R=N+N2P where R is witness for this transaction

    BigInteger Xu = H2(IDu, R).multiply(ss).add(N2);
    //Partial private key Xu = H2(IDu,R)ss +N2

    BigInteger Sk = Xu.add(H1(IDu, N1));
    //Generation of Private Key using algorithm Sk= Xu+H1(IDu+N1)

    ECPoint Pku = Pks.multiply(H2(IDu, R)).add(R);
    //Extraction of public key from available parameters at both end

System.out.println("P = " + P);
System.out.println("Pku (PUBLIC KEY)= " + Pku);
System.out.println("Sk (PRIVATE KEY) = " + Sk.toString(16));
System.out.println("confirmation (P*Sk = Pku) = " + P.multiply(Sk).equals(Pku));
```

Fig 2: Java code for implementation of protocol



```
<terminated> Security [Java Application] C:\Program Files\Java\jre1.8.0_73\bin\javaw.exe (May 12, 2016 7:09:57 PM)
P = org.bouncycastle.math.ec.ECPoint$Fp@ee1d72f4
Pku (PUBLIC KEY)= org.bouncycastle.math.ec.ECPoint$Fp@e9d7f455
Sk (PRIVATE KEY) = 630439251438daa5d8bfd12eb63200cd047a505130c4f7b84ebe3955cbe73cbe3e81502727e7a9af
confirmation (P*Sk = Pku) = true
```

Fig 3 : Result verifying authenticity of code

Authors wrote code to implement above mentioned algorithm using java programming. In this code, they have imported libraries like import java.math, java.security, java.util, org.apache.commons.codec,org.apache.commons.codec.binary, org.bouncycastle.math.ec. As per steps shown in private key generation method, all parameters N, R, X, Sk are calculated respectively as shown in figure 2. At the end, public key calculated. For verification, they have added code showing comparison of public and private keys as per protocol's logic Pk = SP . Results can be seen in figure 3.

5. ENERGY EFFICIENT MODEL FOR PAYMENT APPLICATION

To begin with energy efficient model, there must be a reliable data forwarding structure. Below $'\forall K'$ is the number of bits to be sent in reliable optimal $'RP'$ procedure given as

$$\prod_{i=0}^{\forall K} RP_{ij} \qquad (1)$$

Let us assume that the number of bits for transmission. Bits $'W'$ and size $'S'$ in Kilobytes written as $F(W,E)$ with transmission capacity$'\,T_c'$. This can allow us to calculate the maximum reliable transmission using the following properties

$$T_c = \frac{\theta {\sigma_y}^2}{S{d_x}^{-n}} \qquad (2)$$

Once it begin transmitting using the reliable optimal procedure can be apply it as follows

$$RP : RP_{max} \prod_{(i,j)}^{N} RP_{ij} - RP_{min} \sum_{(i,j\in RP)}^{N} -log \frac{1}{RP_{ij}} \qquad (3)$$

It can further confirm the reliable communication as

$$RP : RP_{min} \sum_{(i,j\in RP)}^{N} -log \frac{1}{RP_{ij}} - RP_{min} \sum_{(i,j\in RP)}^{N} -log^2 - (Wn) - \sum_{(i,j\in RP)}^{N} (-Wn) \qquad (4)$$

Combining the optimal reliable procedure and transmission capacity of Application

$$RP : RP_{min} \sum_{(i,j\in RP)}^{N} -log \frac{1}{RP_{ij}} - RP_{min} \sum_{(i,j\in RP)}^{N} -log^2 - \left(\frac{\theta {\sigma_y}^2}{T_r {d_x}^{-n}}\right) - \sum_{(i,j\in RP)}^{N} \left(-\frac{\theta {\sigma_y}^2}{T_r {d_x}^{-n}}\right) \qquad (5)$$

Once the reliable transmission process has been established next it needs to balance the energy consumption and accuracy of the transmission application. Thus, model also aims to balance the energy utilization for not transmitted bits. With a huge amount of data translation, there is a possibility of the connection dying by transmitting the unlimited amount of data without interval. We define the connection lifetime when the first transmission process is initiated and the consumed energy. Ideally, prolonging the connection lifetime requires satisfying the following conditions:

- Total consumed energy for all transmitted bits should be considered as minimal $'\prod \Delta E_m'$.
- Determining connection-energy consumption for all of the transmitted bits $\Delta E_m (1 \le k \le S_n)$ and an average energy consumption for each transmitted bit $'\Delta E_a'$ is the minimal energy.

By satisfying the conditions, the differences of the energy consumption for all transmitted words and an average energy consumption for single transmitted set of bits is determined by:

5.4.1.1.1.1.1 $\rho^2 = \sum_{k=0}^{n} k\,(\Delta E_m - \Delta E_a)^2$ (6)

where $'\rho^2'$ is the differences between minimal energy and an total energy consumption of the transmitting connection. After determining the differences, we can focus on an average energy ΔE_a consumption for each transmitted text that can be written as:

$$\Delta E_a = \sum_{k=0}^{n} k(\Delta E_m) \qquad (7)$$

With the above equation established we can substitute the value of minimal energy consumption $\Delta E_a$for determining the maximum energy consumption for the all transmitted documents on the connection that can be calculated below.

$$\Delta E_m = \quad \Delta\beta_t \prod_{u\in S(k)}^{n} Y_{uk} + \prod_{v\,\in\,S(k)}^{n} Z_{vk} \qquad (8)$$

We need to determine the number of bits transmitted by connection$'A'$.

$$\omega_p = \left(\Delta\beta_t \prod_{u\in S(k)}^{n} Y_{uk} - \Delta\gamma_r \prod_{v\,\in\,S(k)}^{n} Z_{vk} \right) \qquad (9)$$

Based on the maximum energy consumption and number transmitted bits, the total consumed energy ΔTE_m of the connection can be determined as follows:

$$\Delta TE_m = \sum_{k=0}^{n} k \left(\Delta\beta_t \prod_{u\in S(k)}^{n} Y_{uk} + \prod_{v\,\in\,S(k)}^{n} Z_{vk} \right) \times \left(\Delta\beta_t \prod_{u\in S(k)}^{n} Y_{uk} \prod_{v\,\in\,S(k)}^{n} Z_{vk} \right) \qquad (10)$$

Table 2 : Notations and description for energy efficiency

Notation	Description
$\forall K$	Number of words in the packet to send
W	Bits to encrypt
S	Size in Kbytes
RP	Reliable optimal procedure
Wn	Packets left to send
T_c	Transmission capacity
ρ^2	Difference of individual and average energy
ΔE_m	Minimal Energy Consumed
ΔE_a	Average Energy Consumed
A	Size of packet
$\Delta\beta_t$	Size total data
$\Delta\gamma_r$	Energy Receiving Packet
Y_{uk}	Number of bits encrypted
Z_{vk}	Number of packets encrypted
ω_p	Number of packets sent over network pp

6. ADVANTAGES

6.1. Complete Transaction:

Due payment gateway and server, transaction takes place securely and also it makes sure bank has enough money to complete transaction before initiating as shown in figure 4

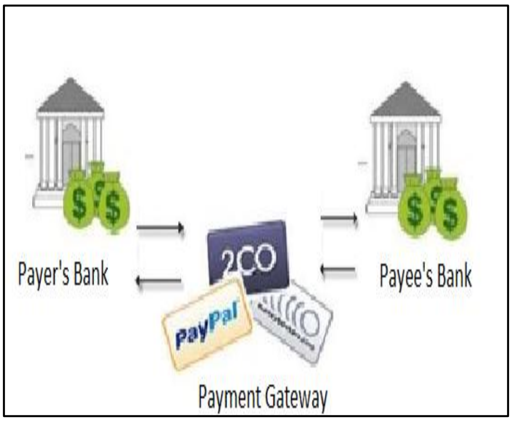


Fig 4 : Safety from impartial transaction

6.2. Pseudo message interference:

Use of encrypted messages can make this protocol more secure and interference of pseudo messages can be avoided.

6.3.Man in middle attack:

As shown in figure 5, private and public key generated from user's input directly. So even if someone tries to impersonate and mislead conversation, they won't be successful.

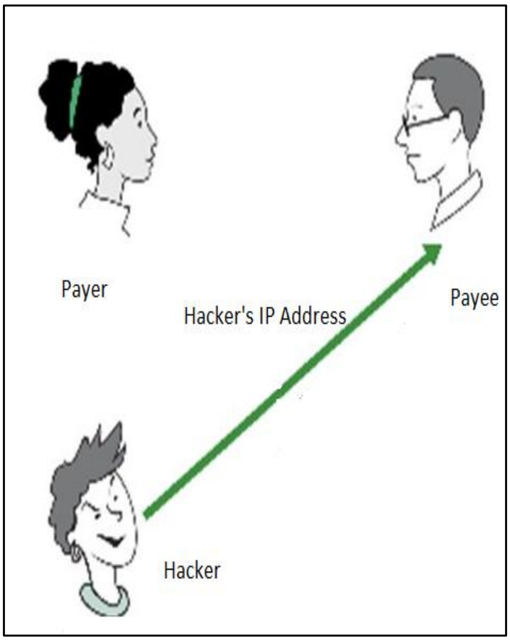


Fig 5 : Safety from man in middle attack

6.4.Confidentiality:

Sender and receivers' identity is only revealed to server, so confidentiality is maintained throughout transaction.

7. CONCLUSION

In this study, Authors have introduced new payment protocol – Self certified key generation payment protocol to increase level of security. Using this method, transactions can become easy and reliable with participation of third party. It increases safety at large extent which would expand E commerce business. Also they have proposed energy efficient model and created the energy efficient algorithm for transmitting data for application. This research paper will be surely useful in future developments in secured payment applications.

8. REFERENCES

[1] C. Kim, K. Changsu, T. Wang, S. Namchul, and K. Ki-Soo, "An empirical study of customers' perceptions of security and trust in e-payment systems," *Electron. Commer. Res. Appl.*, vol. 9, no. 1, pp. 84–95, 2010.

[2] X. Hu, H. Xianpei, L. Wenli, and H. Qing, "Are Mobile Payment and Banking the Killer Apps for Mobile Commerce?," in *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*, 2008.

[3] M. Niranjanamurthy and D. Chahar, "The study of e-commerce security issues and solutions," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, no. 7, 2013.

[4] K. Thompson and T. Ken, "Reflections on trusting trust," *Commun. ACM*, vol. 27, no. 8, pp. 761–763, 1984.

[5] A. K. Jain and S. Devendra, "Addressing Security and Privacy Risks in Mobile Applications," *IT Prof.*, vol. 14, no. 5, pp. 28–33, 2012.

[6] A. K. Ghosh and T. M. Swaminatha, "Software security and privacy risks in mobile e-commerce," *Commun. ACM*, vol. 44, no. 2, pp. 51–57, 2001.

[7] R. A. Botha, S. M. Furnell, and N. L. Clarke, "From desktop to mobile: Examining the security experience," *Comput. Secur.*, vol. 28, no. 3–4, pp. 130–137, 2009.

[8] P. S. Maan and M. Sharma, "Social Engineering: A Partial Technical Attack," *International Journal of Computer Science*, vol. 9, no. 2, 2012.

[9] B. Kraft, E. Mannes, and J. Moldow, "Security Research of a Social Payment App." 2014.

[10] "About Square Cash." [Online]. Available: https://squareup.com/help/us/en/article/5187-about-square-cash. [Accessed: 13-Oct-2015].

[11] Swapna Khandekar, Jingyuan Liang, Abdul Razaque, Fathi Amsaad and Musbah Abdulgader. "Security Research of a Social Payment App and Suggested Improvement". Communications on Applied Electronics 4(5):14-21, February 2016. Published by Foundation of Computer Science (FCS), NY, USA. BibTeX

[12] K. Sahadevaiah, S. Kuncha, and P. R. P.V.G.D., "Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks," *Network Protocols and Algorithms*, vol. 3, no. 4, 2011.

[13] W. Li, L. Wenmin, W. Qiaoyan, S. Qi, and J. Zhengping, "An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network," *Comput. Commun.*, vol. 35, no. 2, pp. 188–195, 2012.

[14] Isaac, Jesus Tellez, Jose Sierra Camara, Sherali Zeadally, and Joaquin Torres Marquez. "A secure vehicle-to-roadside communication payment protocol in vehicular ad hoc networks." *Computer Communications 31,* no. 10(2008):2478-2484.