Indian Journal of Science and Technology, *Vol 10(11), DOI: 10.17485/ijst/2017/v10i11/111087, March 2017*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Hardware Level Security in e-Wallet: Today's Need

Jatinder Singh*

House No. 9, Gali No. 21, Karan Vihar, Karnal, Haryana - 132001, India; jatindersinghsiwach@gmail.com

Abstract

After demonetization in INDIA, eWallets are very actively participating for financial transactions in Indian economy. Very huge population in INDIA, today,is using eWallets. In one side, eWallets are providing very convenience in shopping and online transactions and on another side people are fearing for any online frauds because some eWallets are not following fraud proof security practices, they are using Software security practices like password only. Passwords can sometime be easy breakable or can be stolen online. Hardware level security in various e-Wallets, which are active in INDIA, can reduce these types of frauds. Through hardware level security the e-Wallet would be more secure and can be used freely without worry of fraud. To implement hardware level security measure, application developers have to code applications from scratch. Developers need to find a way so that recoding of application can be avoided.

Keywords: e-Wallets, e-Wallet Security, Hardware Level Security in e-Wallets, Qualcomm's in Mobile App

1. Introduction

The government of INDIA is encouraging the people of country to be cashless. Post demonetization, various steps have been taken by the govt. to encourage for cashless society. To implement cashless society, the govt. is facilitating various tax discount and facilities for cashless transactions[1].

Post 8th November, 2016, there is a huge increase in the daily use of eWallets services like Paytm, Mobiquick etc. by the consumers covering all over country. On the other side, recently, some fraud in Paytm reported. Now, the point begets attention that How much these e-wallets are safe?

2. EWallets and Laws for it in INDIA

eWallets are controlled by RBI in INDIA through Master Circular published on prepaid online payment instruments.

2.1 Master Circular drafted by RBI

1. The criterion and environment to open or operate the eWallets trade in INDIA
2. Ceiling on the amount of money which people of INDIA can deposit in their eWallet accounts,
3. Clash settlement and complaint redressal method for the consumers.
4. Least funds necessities for starting the eWallet business,
5. Provisions for Anti-money laundering.

2.2 Master Circular Does Not Provide

Consumers are in dilemma because it does not set any responsibility in case of fraud that might happen due to faulty security measures.

1. Any minimum standard of security measures which these providers need to abide.

*Author for correspondence

3. Study of Some Security Measures which are Present in eWallet Applications[2]

1. Due to missing of standard in the Indian laws, every wallet company provides its own security measures. Some examples are as below:
2. FreeCharge provides its own patented technology known as "On the Go Pin."
3. Paytm provides password and two factor authentications systems.
4. MobiKwik is providing finger print sensor for iPhones, and two factor authentications to authorize.

But the question is that are above security options are enough?

1. Some other security concerns regarding e-Wallets are as below:
2. eWallets is having third party vendor risk. In today's competitions, each business incorporates other business to achieve its goals, for example travelling company Uber has incorporated Paytm with it. So that, its customers can pay it through Paytm, but if these services are not implemented securely then hackers can have got access to the servers by phishing and can steal user sensitive data.
3. One more example for glitch is that, the financials software, sometimes, do not provide checks before installation on your Smartphone. You can think a scenario in which a user removes or altered the manufacturer provided security in phone then scoundrel app can be mounting in the Smartphone, in this way the malware can simply filch the sensitive information by storing the keystrokes on the phone.
4. There is no policy of these companies which can sense and cure the insiders culprits which expose the security to the persons who have mastery in hacking the services. Secondly, due to lack of technical knowledge, the employees of company can be trapped by technology criminals. These persons can easily fetch important credentials from these employees, can the result is the Risk to customers.
5. No all app of the eWallet have fraud detection team. The main task of these teams is to provide prompt help to the customers which are victim of any financial frauds.

4. Solutions of the Mentioned Problems

Applications must have security features which resolves the above all safety measures, also Applications developers can see the Security model adopted for AliPay (of China), Samsung Pay (of US) and Fido (of Japan) which are using Hardware layered security feature in their app.

4.1 Hardware Level Security

In software base security systems, the companies provide security through special software like Antivirus etc., but as compare to Hardware level security, the security is provided on chip or processor level. Each processed data is encrypted tightly bound to chip or processor[3].

4.2 What it is Exactly?

Senior Director, SY Chowdhary, of Product Management team of Qualcomm also confirmed that financials applications must use hardware layer security, which is built at the chipset level, for eWallets and banking applications. He also have confirmed that their organization reach to app. developers, specially antivirus companies, eWallets and banking applications, and phone makers to make sure that the security of pins and/or passwords is not enough for Smartphones etc., Mr. Chowdhary, also shows that how Qualcomm's secure execution environment can secure the hardware level[4]. This can be seen through Figure 1which shows that hardware level of security comes first and above it, there would be software level security, both security will be provided at the same time.

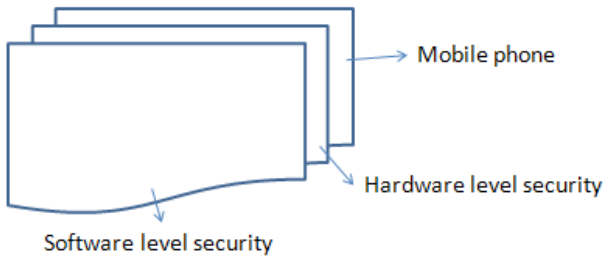

Figure 1. Hardware layer.

4.3 How it Works?

In standard app the security model works as shown in Figure 2.

1. In this, the process is as follows:
2. User provides the password to the app running in Smartphone,
3. The app encrypts this password and send to the server,
4. The server decrypts the password and validates,
5. Response will be sent as per the validation of the password on server.

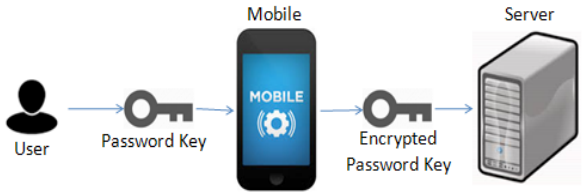

Figure 2. Password based security.

What is threat?

In above scenario, when app is sending the information to server then on the way it may steal and decrypted, if password is weak. And password can be mishandled. It is shown in Figure 3.

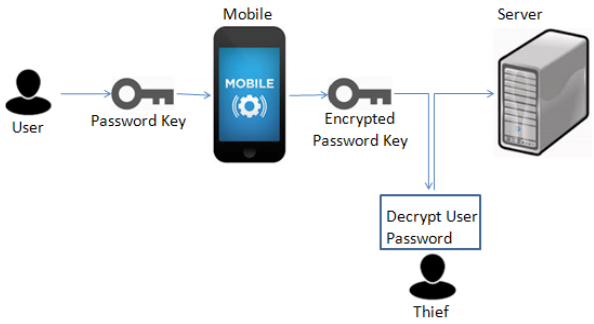

Figure 3. Password based security stolen.

2. Proposed Security Model

Figure 4 shows the process of proposed system. Process is as below:

1. User provides the traditional password with his biometrics like finger prints or any other means like processor number etc. to the app running in Smartphone.
2. App encrypts this information which is called "Hardware Token" and sends to the server.
3. On server end, the server decrypts this information and detect the password and biometric from hardware tokens and compare it with the stored in its memory.
4. If there is a match, then the success result will be conveyed else failed message will have sent.

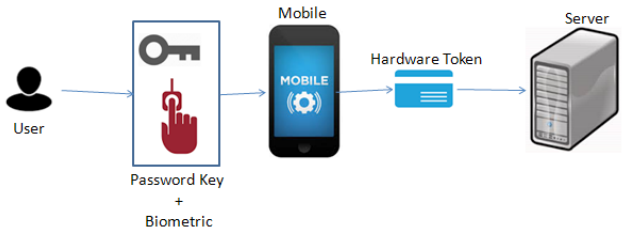

Figure 4. Software and hardware based security.

5. Drawbacks

1. If eWallet companies are willing to adopt this technology then they must develop their software from scratch, so it needs heavy investments.
2. If users' finger prints are not clear then this is a challenge for this technology.

6. Conclusion

By using hardware level security, the chances of fraud and mishandling of finances can be reduced. It is a recent technology and has been used in a few systems. So it needs to fine tuned to the fullest, so that innocent persons can be benefitted.

7. References

1. Introduction [Internet]. [cited 2017 Feb 18]. Available from: Crossref
2. Study of some security measures which are present in eWallet applications [Internet]. [cited 2017 Feb 18]. Available from: Crossref
3. Hardware level security [Internet]. [cited 2017 Feb 21]. Available from: Crossref
4. What it is exactly [Internet]. [cited 2017 Feb 22]. Available from: Crossref.