A SURVEY ON SECURE MOBILE A PAYMENT BY NFC

[1]Shubham Dhamane,[2]Yogesh Jadhao, [3]Rohan Mode,[4]Sahil Gadge, [5]Prof. S.R. Nalamwar
[1,2,3,4]U.G. Student, Department of Computer Engineering, AISSMS COE, Pune, Maharashtra, India
[5]Assistant Professor, Department of Computer Engineering, AISSMS COE, Pune, Maharashtra, India

Abstract-In the current environment, it is necessary to improve security while paying the money. More people than ever before participate in the global economy, largely thanks to the new digital tools available through mobile devices. The increase in digital banking, finance and payments is an important trend that will transform the economies of the world over the next few years. Our scheme provides security against session state reveal attacks and forward secrecy. Usually user store their confidential data for that user need security. Here in proposed system data of user will store in secure form and this data is stored using Aes Encryption algorithm of cryptography. Consumers who use NFC Pay can make secure mobile payments at nearly all merchant locations, via NFC with other mobile that have NFC. Use of near-field communication (NFC) technology through an Android Application to digitally transfer money from the payer's bank account to the payee's bank account with enhanced security and biometric authentication . For security user has to give answers to questions that user has given at the time of registration and also has to give fingerprint that is given at the time of registration. User can done transaction by NFC tag.

Keywords-Digital, Fingerprint, Mobile payment, NFC,NFC Tag

I. INTRODUCTION

As we know Samsung has already announced a strong list of partners that includes MasterCard, Visa, American Express, Bank of America,
Citibank, JPMorgan Chase and U.S. Bank. Samsung Pay users will have access to more merchants than competing mobile payment services, using Samsung's near-field communications (NFC) and secure magnetic
transmission technologies (MST) to support legacy and payment card options. modern Samsung's entry into the smart wallet / mobile payment space comes at an important time in the adoption of mobile commerce and payment.More people than ever are participating in the global economy, in large part due to new digital tools that are available through mobile devices. The increasing no. of digital banking, finance and payments represents a major trend which, over the next several years, that will transform economies worldwide. Security is a main concern for mobile payments, particularly at the point of sale.NFC Pay provides enhanced security with the Samsung KNOX™ mobile security platform and ARM Trust Zone, both of which help protect transaction information from fraud and data attacks.

II. EXISTING SYSTEM

If a person's phone gets stolen and the thief is able to unlock the phone he/ she can use your phone to pay for or to steal money from the payment apps and can access the card information. Also One Time Password (OTP) is send on the registered mobile phone for verification of user, a thief can easily use this OTP to make payments. Biometric identification i.e. fingerprint scan is also not available in many cell phones to make it possible for user to use their fingerprints for payments. In many cases a cell phone is capable of storing more than one fingerprint, and if someone else adds their finger print to the cell phone, they can also use their finger print to make the payment.Samsung Pay is a mobile payment and digital wallet service by Samsung Electronics that lets users make payments using compatible phones and other Samsung-produced devices. The service supports contactless payments using near-field communications, but also incorporates magnetic secure transmission that allows contactless payments to be used on payment terminals that only support magnetic stripe and normal contactless cards.[1]. In countries like India it also supports bill payments.

III. REVIEW OF LITERATURE

A. Worked on When ECC is combined with 3BC, the strength of security is improved effectively . The processing time is substantially reduced. Encryption and decryption time of ECC are much less than those of RSA[1].
Drawback:1.Main disadvantage of ECC is that it increases the size of the encrypted message significantly more than RSA encryption. 2.The ECC algorithm is more complex and more difficult to implement than RSA, which increases the likelihood of implementation errors, thereby reducing the security of the algorithm.

B. Worked on Diffie Hellman does not offer authentication It is less complex than ECC[2].
Drawback:1.Man-in -the-middle Attack possible 2.No Forward Secrecy 3.No key freshness

C. Worked on RSA is two algorithms, one for asymmetric encryption, and one for digital signatures. Works as a block

cipher, where each plaintext/ciphertext block is integer between 0 and *n (for some $n=2^k$)[3]*.

Drawback:1.It never signs a random message.2.Signs Only Hashes.3.It uses different keys for encryption and signature

D. Presented Trusted Execution Environment[11].

issues.2.Security need to enhance.

E. System performing all of the conventional functions of embossed, physically coded, and other forms of magnetic data storage cards [8].

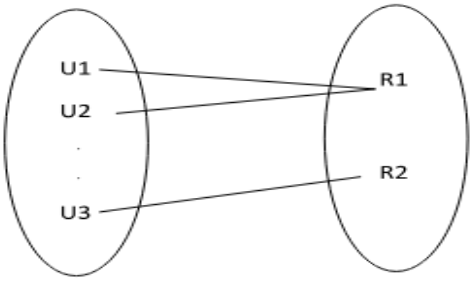
Drawback:1..Security need increase

F. Presented key distribution protocols with timestamps prevent replays of compromised keys[9].

Drawback:1.While sending data through network still security need to enhance.

IV. MATHEMATICAL MODEL:

Set Theory:
S={s, e, X, Y, }
Where,
s = Start of the program.
1. Log in user.
2. Get fingerprint of user
e = End of the program.
1. Login success and nfc device payment success
2. Log out the user.
X = Input of the program.
Input should be amount to pay.
Y = Output of the program.
Finally NFC Payment done success
X, Y U
Let U be the Set of System.
U= {Client, I, S, H, A, D, R}
Where Client, I, S, H, A, D, R are the elements of the set.
Client=User
I=Input data (fingerprint,Amount to transfer).
S=NFC Devices.
H=Hardware.
A=Application (Mobile).
D= select device for payment.
R=Result or output payment done.



Venn Diagram

V. SYSTEM ARCHITECTURE

Proposed System Architecture-

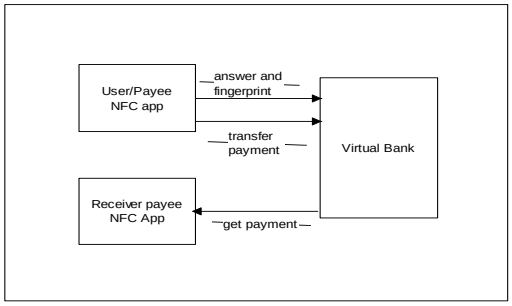


Fig.1: System architecture

System Overview-
Here user login to system.
User will give answer while registering and give fingerprint at the time of registration.
User register his card details in NFC Pay.
User will add money to virtual bank.
User will give answer to asked question in nfc pay while paying money.
User will give fingerprint and then pay money.
User will view his transaction.
User can done transaction by NFC tag
Advantages-

A. Grant access to authorized users
B. Prevent exposure of user related data (privacy)
C. Secure communications between device and backend.
D. Ensure system integrity.
E. Protection of credentials.

CONCLUSION

Proposed system will used for payment transferring system. It uses Samsung NFC Feature. Use of near-field communication (NFC) technology through an Android Application to digitally transfer money from the payer's bank account to the payee's bank account with enhanced security and biometric authentication . Consumers who use Samsung Pay can make secure mobile payments at nearly all merchant locations, via NFC. User pay payment by NFC Tag.

REFERENCES

[1]. Byung kwan Lee, Tai-Chi Lee, Seung Hae Yang, "An ASEP (Advanced Secure Electronic Payment) Protocol Design Using 3BC and ECC(F2m) Algorithm", 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'04), pp. 341 – 346

[2]. Ian F. Blake, Theo Garefalakis, "the complexity of the Discrete Logarithm and Diffe-Hellman problems", *Journal of Complexity*, vol. 20, pp. 148-170, 2004.

[3]. M. Thangavel, P. Varalakshmi, Mukund Murrali, K. Nithya, "An Enhanced and Secured RSA Key Generation Scheme" in

Department of Information Technology Anna University, Chennai:Elsevier, 2014

[4]. Svigals, J.; Ziegler, H.A., "Magnetic-stripe credit cards: Big business in the offings", Spectrum, IEEE, 1974, Volume: 11, Issue: 12

[5]. Smith, D.F.; Donnelly, T.; Mapps,D.J., "The credit card as a mass storage medium", IEE Colloquium on Document Image Processing and Multimedia Environments, 1995

[6]. ISO/IEC 7813 Standard information technology -- Identification cards -- Financial transaction cards

[7]. Roland, M., "Applying recent secure element relay attack scenarios to the real world: Google Wallet Relay Attack", technical report, August 2012.

[8]. Svigals, J.; Ziegler, H.A., "Magnetic-stripe credit cards: Big business in the offings", Spectrum, IEEE, 1974, Volume: 11, Issue: 12

[9]. D. Denning and G. M. Sacco, "Timestamps in key distribution protocols," *Commun. ACM*, vol. 24, no. 8, pp. 533–536, 1981.

[10]. K. Nyberg and R. A. Rueppel, "Weaknesses in some recent key agreement protocols," *Electron. Lett.*, vol. 30, pp. 26-27, Jan. 1994.

[11]. Urien, Xavier Aghina, Pascal " Secure Mobile Payments Based on Cloud Services: Concepts And Experiments." 2016 IEEE