SECURITY OF MOBILE PAYMENT SYSTEMS: A REVIEW

Aditi Pathak[1], Sanjay Silakari[2], Anjana Jayant Deen[3], Rajeev Pandey[4]

[1] Student, [2] Professor, [3] Assistant Professor, [4] Assistant Professor,

Department of Computer science and Engineering, UIT, RGPV, Bhopal (M.P)(India)

ABSTRACT

Smart devices play major role in electronic payments transaction. Smart phones have gone beyond the call of duty, as businesses and banks are now leveraging the Internet of Things (IoT) to expand their reach and offer a fast and convenient service to consumers. The mobile payments reduce the cost of traditional payments transaction but face a severe problem of security threats. The process of mobile payments system used the internet and communication medium which can be compromised with security attacks resulting into finical frauds and many illegal behaviors over the payments. In this paper we present the review of mobile payments system using secured communication and transaction system. The capabilities and limitations of mobile devices introduce some challenges for designing effective and efficient authentication mechanisms.

keywords :- Cryptography, Key Management, Mobile Agents, Payment Security, QR code.

I. INTRODUCTION

Due to recent advancements in technology, there is a rapid increase in use of mobile devices for making payment transactions. Security of private data stored on the smart phone has become increasingly important as more and more users and businesses use smart phones not only for the purpose of communication but also as a means of planning and organizing their work and private life [1,2]. Smart phones are the most picked target of attacks. These attacks exploit weaknesses related to smart phones that can come from means of communication like SMS, MMS, Wi-Fi networks, and GSM. These attacks also exploit software vulnerabilities from both the web browser and operating system. Also weak knowledge of average mobile user gives a scope to malicious software. Different security counter-measures are being developed and applied to smart phones, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps [3]. Several implementations have emerged as the key methods to use a cellular phone in remote network authentication. The following Fig.1 gives the various steps involved in a mobile payment system.

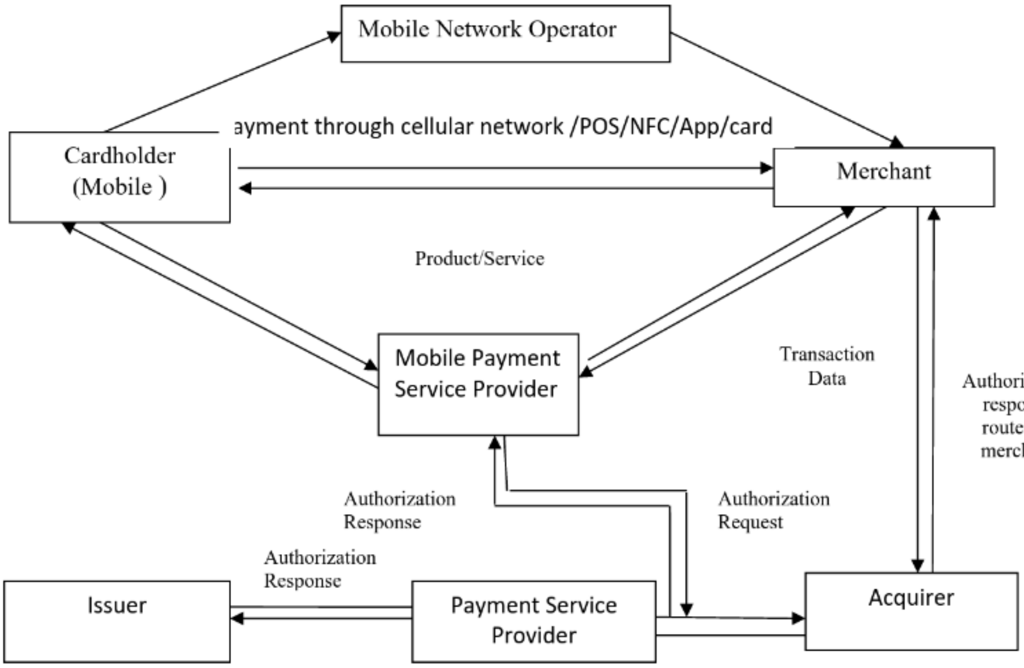


Figure.1 architecture of mobile payment system

1.1 Mobile Agents

A mobile agent is a combination of a computer software and data which is able to migrate from one system to another freely and also persist its execution on the destination computer. It is therefore a process that can freightage its state from one environment to another. Mobile agents can be of two types depending upon their migration path. They are of autonomous nature and therefore are suitable for developing mobile application as they use less of network bandwidth compared to RPI or RMI (Java) and can display better response time. After arriving at the destination the mobile agent responds faster. Use of mobile agents have several advantages like computational bundles , simultaneous processing, dynamic adaptation, tolerance for new faults, easy/flexible maintenance and reduction in compilation time. An agent is therefore a simple building block for design of multi agent systems. A new computing paradigm is exhibited by the mobile agent technology where in a program delays its execution on the host computer and transfers itself to other agent enabled host on the same network and continue its execution on this new host. However there are many security issues faced by the developers of mobile agent. The main threat related to mobile agents system is security especially when there is a need to deal with soft/digital cash. [4]

1.2 Payment Protocols

A. SET (Secure Electronic Transaction)

It is a security protocol that facilitates users to apply the alive credit/debit card payment infrastructure on the internet in a secure manner. For all the parties involved a secure communication channel is provided. It also caters authentication by the use of digital certificates. This process ensures confidentiality. The set model is explained in Fig.2.

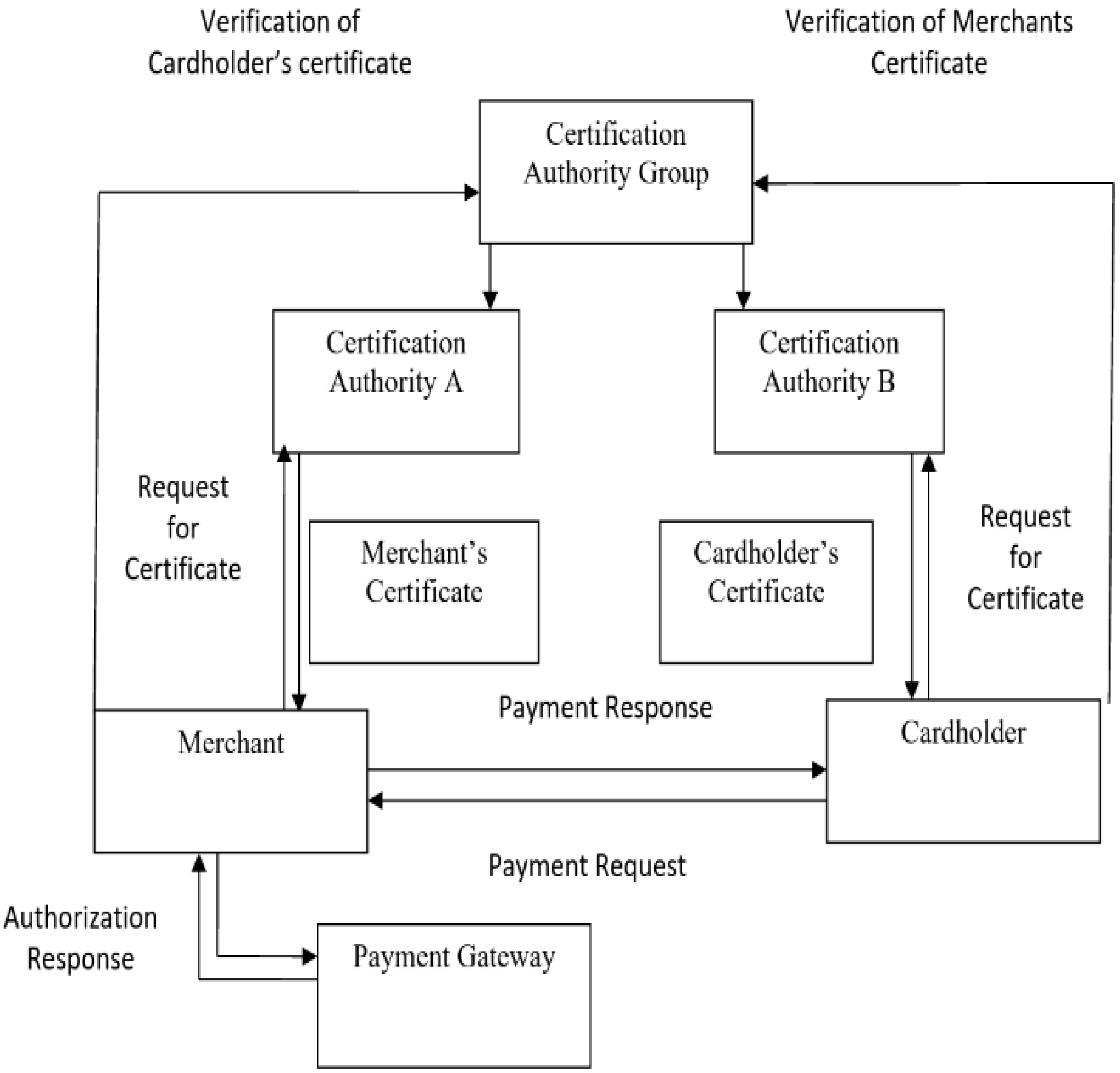


figure.2 SET model

There are 6 key players in an electronic transaction:

Cardholder: He is the sanctioned owner of a payment card such as MasterCard or Visa that is provided by a issuer .

Issuer: The financial institution that provides a payment card to the cardholder, and is eventually accountable for the payment of the cardholder's debt.

Merchant: A person or an organization who wishes to provide goods and services to the cardholder using electronic means.

Acquirer: This financial institution is related to the merchants for processing payments cards authorizations and payments. It also provides electronic funds transfer to the merchant account.

Payment Gateway: It acts as an interface between SET and existing card payment network.

An attractive aspect of this process is the use of dual signature (represented in Fig.3) which certifies that the merchant and the payment gateway access only the information that they require, and this eventually protects the card details of the cardholder.

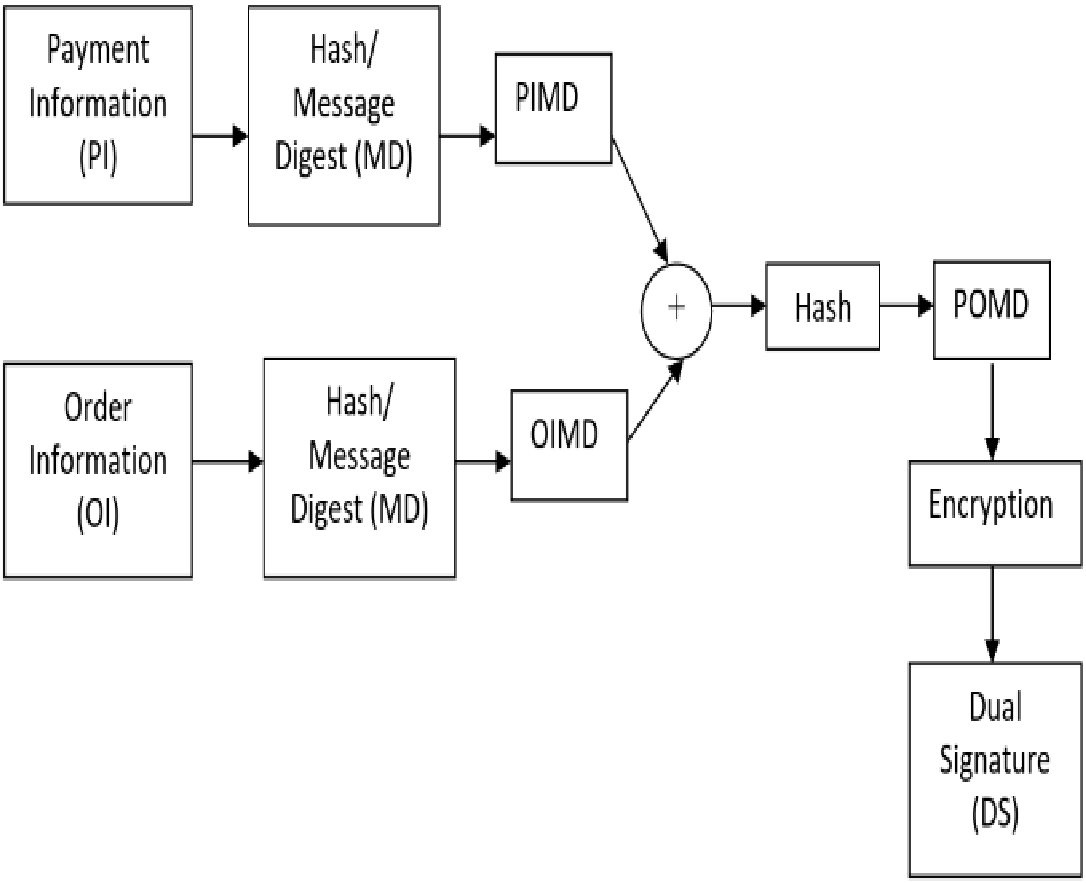
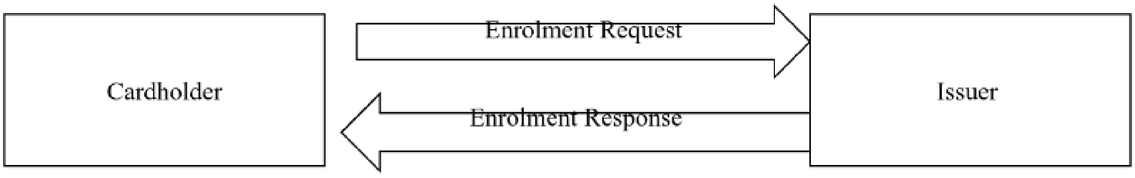


figure.3 dual signature

Despite of its benefits SET has restrictions as well, it does not prohibit misuse of card details, which is although abstracted from the merchant, by false user.

B. 3-D (Three Dimensional) SECURE

It is a protocol based on XML devised to indulge additional security layer for online card transactions. The key approach of this protocol to link the financial authorization process with an online authentication. As the name suggests it is based on a model of 3 domains namely, Issuer, acquirer, and interoperability. Messages are transmitted over SSL connection with client authentication. Any cardholder who wishes to participate in a payment transaction involving this protocol has to first enroll itself(depicted by Fig.4) on the issuer's bank enrollment server. Figure 5 shows the working diagram of 3-D
secure



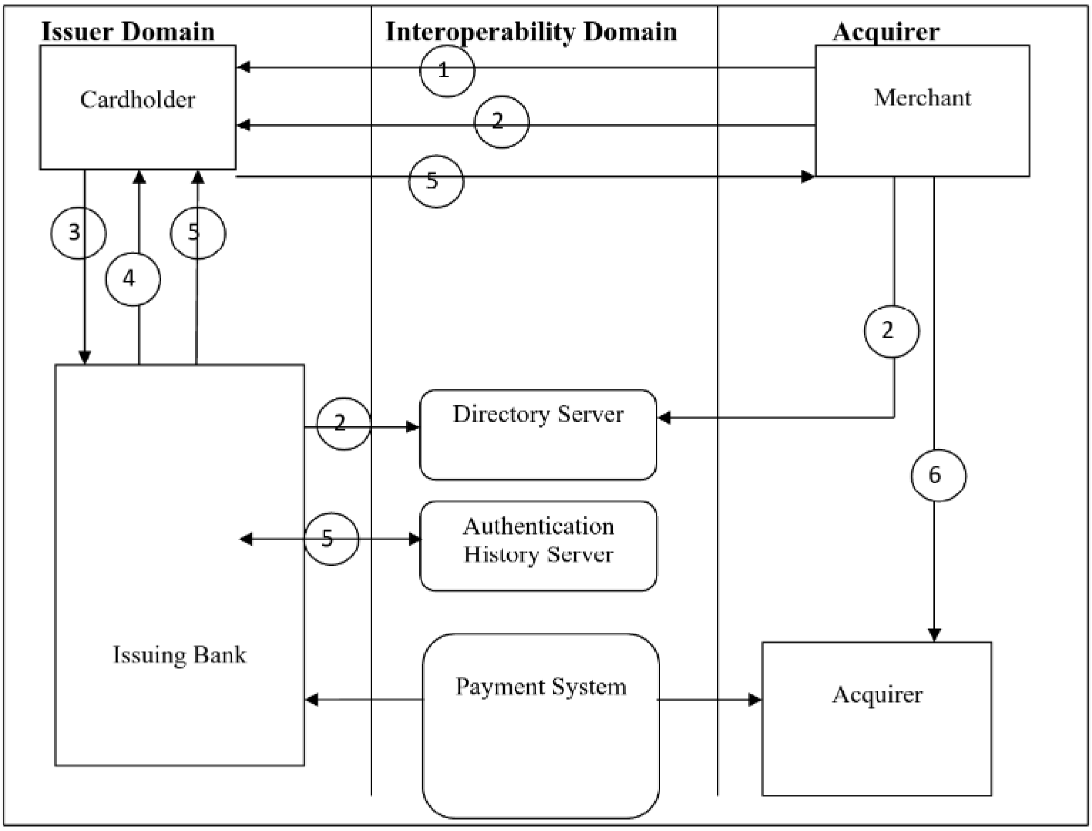


Figure.5 Internal Flow Diagram of 3-D Secure

1.3 One Time Password (OTP)

An OTP is a single use symmetric key that is used for encryption of all the messages in one communication channel. They are used to dodge the drawbacks related with conventional password based authentication .Their most important edge is that they are not vulnerable to replay attacks. Smart phones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company. One such solution focuses on using cellular phone as a standalone OTP token [5]. The phone is a computational platform to generate the OTP code. The OTP generating software, user’s secret seed and counter value are stored in the cellular phone. In operating the token, the user activates the software. The phone generates the OTP code. The user reads the OTP code and enters it into a PC or Internet device for 2FA need. Once authenticated, the user is allowed to access the network. these simple mobile tokens usually do not have any capability to resist the OTP seed (K) tracing by MITM interception or Shoulder-surfing attacks. Moreover, it stores the secret seed and counter value however these secrecies can be exposed if the phone is lost or stolen [6,7].

1.4 QR (Quick Response) Code

QR code is an optical machine readable 2-dimensional code which represents an information concealing technique. It offers fast readability and greater storage capacity.

Blocks of squares arranged in a square grid on a white background that is read by an imaging device such as camera and processed by using reed-solomon error correction until the image can be approximately interpreted. Later on the required data is extracted from patterns that are presented in both horizontal and vertical components of the image. This technique ought to be utilized to guarantee that the data is right and is gotten or sent by confirmed gathering. In this paper, Encrypted QR Code through PKI is examined for securing data in the portable installment framework. Securing encryption key needs trusted-outsider that has obligations to guarantee that both sides are genuine clients [8,9]. The public key encryption techniques reduce the security risk of mobile devices payments system. The public key encryption techniques provide various key authentication and authorization process for the secured electronic transaction [10,11].

1.5 Key Generation

Key management is the set of techniques that involves generation, distribution, storage, and revoking, verifying keys.The taxonomy of generation of keys is shown in figure 6. When there are multiple users key management system (KMS) has to create separate key for each user and distribute it to them If the key is crashed KMS has to recover the key. If it is not being used then KMS has to delete the key. Key is associated with metadata. Metadata contains information about key label, key identifier, key life cycle, cryptographic algorithm and parameters for the key, length of the key, key usage count. Key life cycle contains various states such as reaction, initialization, full distribution, active , inactive and termination. Figure 7 depicts the management of key at server and client side.

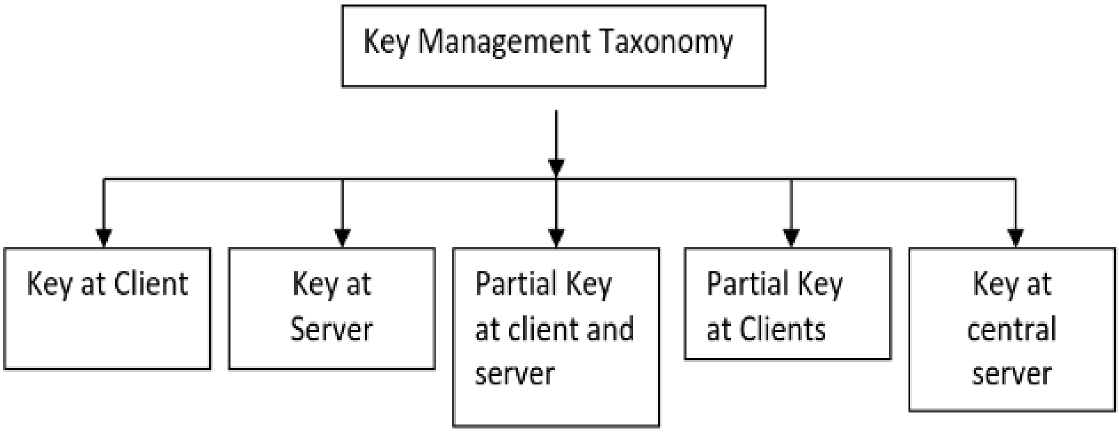


Figure.6 Taxonomy of key generation technique.

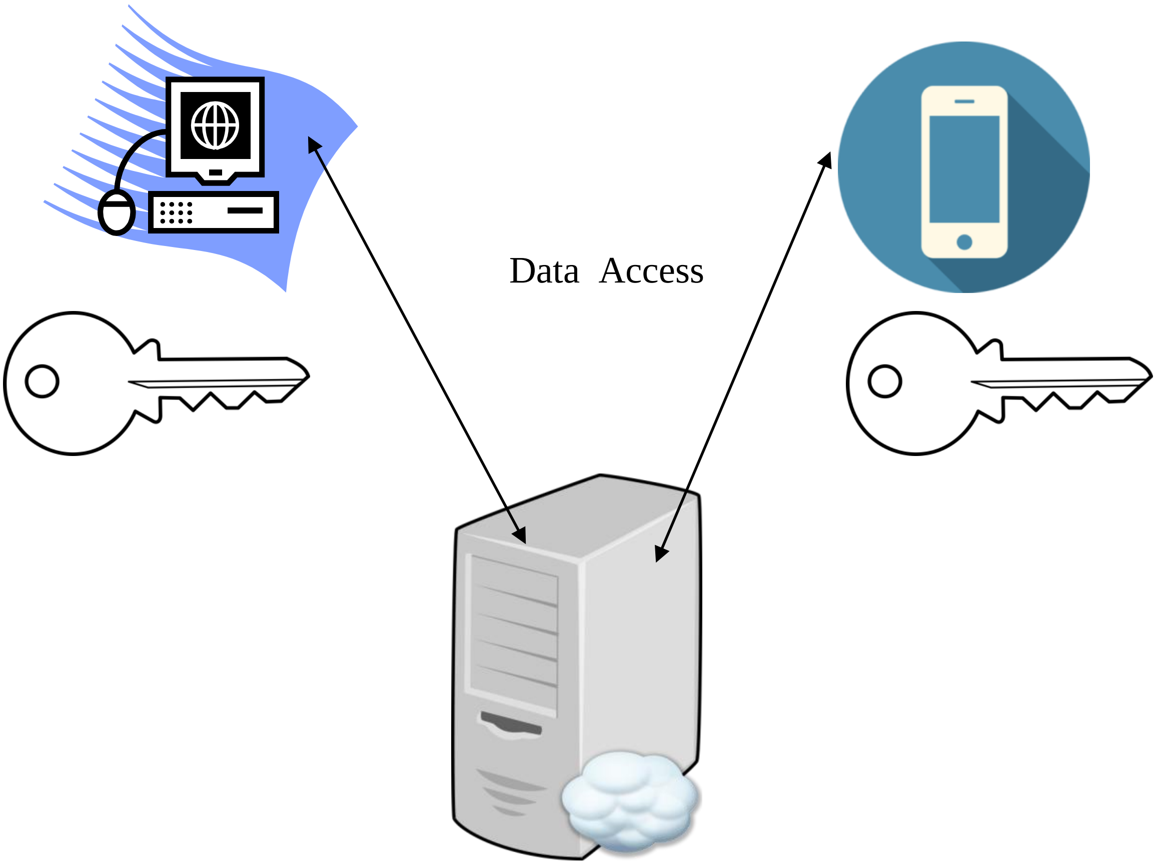


Figure.7 Management of keys at client and server side

1. MANAGEMENT OF KEY AT CLIENT SIDE

In this approach, data will be stored at server side in encrypted form. Client may be thin e.g. mobile phone. Keys will be maintained at phone user and desktop side. Usually this approach is taken in Homomorphism cryptographic technique. Operations are done on encrypted data at server side [9,12].

2. KEY MANAGEMENT AT SERVER SIDE

In this approach, keys are maintained at server side. If the key is lost, customer is unable to read data which is present at server. Data is stored in the encrypted form and can be only decrypted by the key in order to get it in the original form[13].

3. MANAGEMENT OF KEY AT BOTH SIDES

In this technique, key is divided into two parts. One part is stored at user side and other part is stored at the server side. If both parts are combined together, it is possible to retrieve the data properly. Thus, data remains secure and can be controlled by the user. Thus, solution is also scalable. Server and user do not need to maintain complete key at server side. If part of the key is lost, data cannot be recovered[14].

1.6 Problem Formulation

The multiplication of Mobile devices, for example, Mobile phones and tablets not just gives purchasers more decision; it additionally can possibly extend the installments to bringing new players, for example, versatile administrators and handset makers in with the general mish-mash. Numerous installment supporters are vying for consideration, with each gathering propelling an alternate vision for where the purchaser's electronic wallet the confided in wellspring of certifications ought to dwell, on a card, on a telephone, or in the Cloud [13,14]. These different methodologies make new difficulties and at times can possibly set up new plans of action. The conventional part of banks in issuing physical cards that are sent to clients could be supplanted by new classes of middle people, for example, Trusted Service Managers (TSMs) that give over-the-air provisioning abilities to Mobile phones. Following point consider as security risk[15,16]

1. Inability to adjust to portable installments can put your organization at a focused hindrance.
2. New forms make new security vulnerabilities. Over-the-air provisioning of installment qualifications and applications, for instance, conceivably makes new assault vectors for busybodies to take and abuse client information.
3. Attackers can take and abuse information, prompting excruciating revelations, antagonistic reputation, and fines.
4. Failure to see precisely where and how delicate record information is put away and transmitted can keep associations from plainly characterizing and executing information security arrangements.
5. Rising exchange volumes can prompt execution bottlenecks as wasteful handling limits limit and corrupts the client encounter [16].
6. Overly awkward and expensive security plans can thwart an association's capacity to adjust rapidly to new open doors or to scale its business procedures to take care of rising administration demand[17].]

II. LITERATURE SURVEY RELATED WORK

Title	Approach and Result
Authentication in mobile cloud computing: A survey[1]	The results of the evaluation show that some important factors such as user preferences, mobility, het-erogeneity, mobile device characteristics, and MCC-friendliness are highly critical to be considered when designing the future authentication mechanisms for MCC. It is also suggest that the most appropriate authentication method in MCC would be hybrid adaptive methods with varied degrees of fidelity that can be adopted depending on user location, Internet connectivity, native resource level, and remote resource proximity.
Smartphone Base D Secure Color Qr Code Using Visible Light Communication[2]	This paper discusses a two-phase scheme for transferring message between two smart phones. Finally, they can get their resultant graph by means of frame decoding rate.
Authentication in mobile cloud computing by combining the two factor Authentication and one time password token[3].	This paper presents an authentication mechanism in mobile cloud computing with combining the two-factor authentication and one time dynamic password called OTP token that suitable for mobile device. As they have shown a strong authentication system and well resist against seed tracing, MITM-seed

	tracing and shoulder surfing attacks.
Bring Your Own Device For Authentication (BYOD4A) – The Xign–System[5]	To enable the authentication of users by using their personal devices, the authentication system needs to be designed to be flexible. Ideally the system does not depend on passwords, as the problems regarding that type of authentication are well-known. Most passwords are either easy to guess or, if password policies are in effect, not easy to remember. Systems that are not easy to use, typically won't be used as frequent as their easier, maybe more unsafe counterparts.
UbiKiMa: Ubiquitous authentication using a smartphone, migrating from passwords to strong cryptography[6]	This paper discusses that a working prototype needs to be stream-lined and tested. Then, actual deployment needs to be encouraged. This step will focus on getting as many users as possible to adopt the smartphone app as a convenient and ubiquitously usable password manager. Parallel to that, integration support for service providers in terms of API's and proper documentation will be developed. Finally, key management protocols need to be developed, and secure backup strategies for key material need to be integrated.
A Secure Operational Model for Mobile Payments[7]	This paper looks upon authentication, confidentiality, and integrity, nonrepudiation and privacy. The encryption and decryption processes are not performed on mobile devices, which eliminate the problem of some mobile devices being unable to support powerful cryptographic algorithms. The discussed platform based on a web-services architecture is extensible, inexpensive, and easy to configure
A Mobile Payment System With an Extra Token of Security[8]	This paper introduces a new Authentication Factor that is called by Two-Factors Authentication Plus, (2FA+). Mobile Payments are becoming a feature that more and more people are using. This has resulted in more sensitive financial data are being stored on these mobile devices.
Mobile Payments: Merchant's Perspectives[9]	This article finds two attributes with clear effects on merchants are customer shopping experience and fragmented markets. Mobile payments will provide benefits to merchants through customer shopping experience.
Mutual Authentication in Securing Mobile Payment System using Encrypted QR Code based on Public Key Infrastructure[10]	This paper addresses the issue of mutual authentication to ensure the security of the transaction. The third party does this mutual authentication through PKI system. Using this Public Key Infrastructure will keep the key distribution secure, ensure sender and recipient as a legitimate user and

	guarantee that the data information is confidential. This encryption system using RSA algorithm which is trusted as strongest asymmetric encryption system.
Augmented Reality based Smart City Services using Secure IoT Infrastructure[11]	The work presented in this paper is focused on implementation of novel smart city service within the public transportation powered by the Augmented Reality (AR) technology. . Overall system is presented with the focus on the security aspects to be addressed within the system. Description of the complete end-to-end solution is presented, providing the overall system set-up, user experience aspects and the security of the overall system, focusing on the lightweight encryption used within the low-powered IoT devices.
SWEP Protocol and S-Wallet System - Mobile Payments using Near Field Communications[12]	The S-Wallet system discussed in this article uses the Android SDK based on JAVA. The main advantage of S-Wallet system compared to systems currently developed is that the integration between the S-Wallet Account, the App and SWEP protocol provided more security and speed for the transaction of mobile payments.
Mobile Authentication with German eID[13]	The security evaluation showed, that no harmful attacks could be executed, which means that neither the eID token nor the cryptographic keys were compromised. It’s possible to transfer the described concept to eID solutions of other countries as long as a sovereign service provider managing the eID tokens is available and the processes are compliant with the law.
Secure Data Storage in Mobile Cloud Computing[14]	This paper has provided the description about the basics of Mobile Cloud Computing and issues associated with it. Mainly it discussed about security of data stored in cloud and importance of data security. It also discusses a mechanism to provide confidentiality, access control as well as integrity to mobile users.
E-payment Security Analysis In Depth[15]	This paper makes use of SSL technology which is the safest mechanism being used today or another secure method. Users who see the yellow padlock at the bottom of the browser may get a false sense of security.
Hybrid Attribute-Based Encryption and Re-Encryption for Scalable Mobile Applications in Clouds[16]	The discussed protocol in similar in overall performance to the original ciphertext-policy attribute-based-encryption idea, while significantly lessening the computational and traffic burden on the mobile data owner. Thus, the discussed is useful for securing mobile cloud computing with very

	large user populations.
Secure Ciphering based QR Pay System for Mobile Devices[17]	Discusses use of an innovative mobile payment system based on QR codes for mobile users to improve experience in conducting mobile payment transactions. they find that information sent/received to the Payment Gateway(PG) is not encrypted which is susceptible to relay or spoofing attacks. So to replace this plain message sharing with ciphered messages that use a robust secure ciphering technique such as AES or DES algorithm.
NFC based mobile payment protocol with user anonymity[18]	This paper describes the use of Virtual Transaction Account in order to anonymize the identity of the payer . Also time stamp is appended after each transmission. It makes the use Diffie Hellman key exchange in order to generate a session key .The described technique makes it impossible for linkability of user account and valso is resistant to replay attacks
A Secure SMS Protocol for Implementing Digital Cash System.[19]	This paper introduces a protocol in order to implement digital cash by using a set of static and ephemeral public keys that are used to derive a fresh shared key for each transaction. There is use of Elliptic Curve Menezes-Qu Vanstone *(*ECMQV*)* Key Agreement for that purpose. The proposed method provides protection against cryptanalysis attacks at low communication cost.
Secure Mobile Payment on NFC-Enabled Mobile Phones Formally Analysed Using CasperFDR.[20]	This paper tries to address the issues of NFC that is loss of security and privacy by using the OTP to generate secret session keys that encrypt the customer’s data. It makes use of Hash of the PIN (HPIN) to generate the OTP. The result of the described technique is that is preserves tag’s data privacy and also provide mutual authentication.
Design of Secure Mobile Payment System Based on IBC.[21]	This paper focuses on preventing the tampering of transactions by adding an IB-signature along with the communication data in transactions, and using the "one-time key" mechanism to encrypt the data of transactions . It describes the use of Identity-Based Cryptography (IBC) also ensuring non-repudiation of information.

Secure mobile payment based on Super SET protocol.[22]	This paper introduced an enhanced version of Set protocol to address the security principles of integrity , confidentiality of sensitive information and transaction atomicity. It also explains the adoption of the advanced mechanism, the credit hierarchical system, the dispute arbitrate mechanism and the virtual user information system.
Enhanced Mobile SET Protocol with Formal Verification.[23]	This paper defines the use of Set protocol along with PKI for both online as well as offline mode, also withstanding attacks like replay and impersonation. It makes use of mobile agent technology, digital signature with message recovery (DSMR) and elliptic curve digital signature algorithm (*ECDSA*)
EMV-TLS, a Secure Payment Protocol For NFC Enabled Mobiles.[24]	This paper concentrates on remotely handling a EMV device from a server. Establishing a secure channel (i.e. TLS connection) between an EMV chip and a Payment Service Provider. It explains merging of three technologies: EMV payment applications, SSL/TLS secure channels, and Near Field Communication radio interfaces. It defines a trustworthy remote use of a chip.

III. CONCLUSION AND FUTURE SCOPE

The mobile payment systems used various key authentication and authorization processes. For the authentication and authorization there is use of public key infrastructure and QR code technique. The mobile payment system also use the concept of third party payment transfer system. The third-party transfer system use the process of cloud auditing. In the process of survey, we also studied various security threats on smart device payment system. Some security threats such as traffic attack, fake OTP , profile updating, open wallet and many security attacks. For the minimization of security risk QR code scanning process is used for the mobile payments systems. In future , the use of hybrid, asymmetric cryptography technique can be helpful for securing mobile payments.

REFERENCES

[1] Mojtaba Alizadeh, Saeid Abolfazli, Mazdak Zamani, Sabariah Baharun and Kouichi Sakurai “Authentication in mobile cloud computing: A survey”, Elsevier, 2016.

[2] R.SHARMILA and M.MOHAMED SITHIK “Smartphone based secure color qr code using visible light communication”, IJARBEST.

[3] Najmeh Mashhadi “Authentication in mobile cloud computing by combining the two factor Authentication and one time password token”, Ciência e Natura, 2015.

[4] M. Malathy, S. Jasmine Smilee, J. Niranjan Samuel “Secure mobile agent in M-Commerce over internet”, IEEE, 2016.

[5] Norbert Pohlmann, Markus Hertlein and Pascal Manaras "Bring Your Own Device For Authentication (BYOD4A) – The Xign–System", Springer, 2015.

[6] Maarten H. Everts, Jaap-Henk Hoepman and Johanneke Siljee "UbiKiMa: Ubiquitous authentication using a smartphone, migrating from passwords to strong cryptography", ACM, 2013

[7] Tao-Ku Chang "A Secure Operational Model for Mobile Payments", Scientific World Journal, 2014.

[8] Nael Hirzallah and Sana Nseir "a mobile payment system with an extra token of security", International Journal of Computer Engineering and Applications, 2014.

[9] Fumiko Hayashi and Terri Bradford "Mobile Payments: Merchants' Perspectives", federal reserve bank of kansas city, 2014.

[10] Ariana Tulus Purnomo, Yudi Satria Gondokaryono and Chang-Soo Kim "*Mutual Authentication in Securing Mobile Payment System using Encrypted QR Code based on Public Key Infrastructure", IEEE, 2016.*

[11] Boris Pokrić, Srđan Krčo and Maja Pokrić "*Augmented Reality based Smart City Services using Secure IoT Infrastructure", IEEE, 2014.*

[11] S. H. V. C. Silva, E. L. Flôres, G. A. Carrijo, A. C. P. Veiga, and M. B. P. Carneiro "SWEP Protocol and S-Wallet System - Mobile Payments using Near Field Communications", Hindawi, 2014.

[12] Florian Otterbein, Tim Ohlendorf and Marian Margraf "Mobile Authentication with German eID", arXiv, 2017.

[13] Preeti Garg and Dr. Vineet Sharma "Secure Data Storage in Mobile Cloud Computing", International Journal of Scientific & Engineering Research, 2013.

[14] Adam Ali.Zare Hudaib "E-payment Security Analysis In Depth", IJCSS, Pp 2014.

[15] Piotr K. Tysowski and M. Anwarul Hasan "Hybrid Attribute-Based Encryption and Re-Encryption for Scalable Mobile Applications in Clouds", IEEE, 2013.

[16] V.N.V.H Sudheer and J.Ranga Rajesh "Secure Ciphering based QR Pay System for Mobile Devices", International Journal of Emerging Trends in Engineering and Development, 2013.

[17] Shang-Wen Chen and Raylin Tso, "NFC-based Mobile Payment Protocol with User Anonymity", IEEE, 2016.

[18] N.Raghu Kisore and Supriya Sagi "A Secure SMS Protocol for Implementing Digital Cash System", IEEE, 2015.

[19] Sarah Abughazalah, Kostantinos Markantonakis and Keith Mayes , "Secure Mobile Payment on NFC-Enabled Mobile Phones Formally Analysed Using CasperFDR", IEEE, 2015.

[20] YANG Rui-xia, "Design of Secure Mobile Payment System Based on IBC", IEEE, 2016.

[21] WAN Zhongbao and Wang Qing, "Secure mobile payment based on Super SET protocol", IEEE, 2010

[22] Shaik Shakeel Ahamad, V.N.Sastry and Siba K. Udgata2, "Enhanced Mobile SET Protocol with Formal Verification", IEEE, 2013

[23] Pascal Urien, "EMV-TLS, a Secure Payment Protocol For NFC Enabled Mobiles", IEEE, 2014.