International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

# Recent Advancement in Mobile Payment Security Systems

**Deepika Dhamija, Anu Bharti**

***Abstract:*** ***The recent advancements in Information Technology have brought considerable changes in the way tasks are accomplished across the globe. The world has become a more connected place and a major impact as well as reason of this can be attributed to the steep rise in the usage of mobile devices. Mobile devices are being used for online payments in the form of shopping, money transfers, bill payments and what not. The majority of monetary transactions on the Internet now take place through mobile devices and therefore, mobile payment systems being wireless systems calls for an even more secure protocols and payment environment. Although the various security protocols available today boast of implementing the security requirements i.e. data confidentiality, integrity, non-repudiation, authentication and authorization, still the security of m-commerce transactions remain a major concern for mobile payment users. A number of m-commerce security techniques, models and protocols have been proposed by authors in recent past. This paper presents the recent advancements of the models and techniques authors proposed and the technologies and protocols used in these models. The paper also highlights the open areas of research in the field.***

***Keywords: Mobile, Commerce, M-Commerce, Security, Protocol, Payment, Network***

## I. INTRODUCTION

M-commerce or mobile commerce is the buzz word in the present era where the organizations are focusing on creating a business model that can deploy and reap benefits of this opportunity. To be specific, M-commerce (mobile commerce) can be defined as trading of products and services with the help of handheld devices like mobile phones, smart phones and other smart devices [1]. The distinctive feature of m-commerce is that the users can access and use it from anywhere, any location with the availability of mobile data on their smart devices. The users as well as the service providers have realized that m-commerce is here to stay and therefore, everyone seems to be determined in unleashing the features those m-commerce offers. The rise in m-commerce platform is evidenced from the fact that in 2017, the number of mobile payment users stood at 52.9 million while in 2019, it reached at 93.3 million, according to a report. Thus, there is no doubt that M-commerce is helpful in making our life much easier for today's generation where there is no need to remain connected with network cables and wires and any kind of activity that is being carried out through mobile devices is purely wireless, thanks to the advancements in Information technology, Telecommunication networks. The mobile users can enjoy their shopping, the employees are doing their office work from the convenience of their homes, but this convenience comes with a price. The most important aspect here is the security of the mobile payment network and to ensure that the monetary transactions are carried out without any risk of security breach like passive attacks, eavesdropping, and loss of private information. All these security threats have happened in the past and thus, even though the mobile users are using mobile devices for online payments and shopping, they always remain under constant threat of data loss or a security breach.

Mobile commerce disposed the passive attacks and on-going conversation with the help of radio frequency. Customers have numerous concerns about the information which they share with participating parties i.e data or voice messages or both from unauthorized party gaining access. Alternatively identification integrity and message integrity are also the part of mobile security. Unhappily, when it comes to online transaction, mobile communication doesn't offer full security measures. For a safe and secure M-Commerce system, the following services should be considered.

1. Authentication- It is the process of verifying and validating the credentials of a user or mobile client who possesses the mobile device. Both the mobile client and the merchant need to prove their identities to each other before the transaction are initiated [2].

2. Confidentiality- It is the process of ensuring that the data and message traveling over the untrusted network remains safe and secure. Ensuring confidentiality is of prime importance as if this is compromised, the sole purpose of conducting the online business gets over. The unauthorized users shouldn't be able to access and see the transaction details [3].

3. Integrity- It is the process of ensuring that the message contents are not tampered or shared with unauthorized users during its transmission [3].

4. Non-Repudiation-This process is carried out to ensure that both the sending and receiving parties cannot deny of having participated in an online communication [4][5].

Diverse systems of making payment through mobile devices have developed in recent years that let the mobile payments take place in a seamless and secure manner. To secure payment through mobile various new models have been proposed by various authors. In this review paper, the focus is on analysing the various proposed models and what technologies and protocols have been used in the models.

Revised Manuscript Received on December 30, 2019.

* Correspondence Author
**Ms. Deepika Dhamija*,** Assistant professor, Amity University Haryana, India.
**Dr.Anu Bharti,** Dean of Engineering, Sunrise University Alwar, Rajasthan, India.

The remaining paper is structured as per the following sections: Section 2 presents the review method where research questions are formulated and stepwise review process is explained. Section 3 presents the detailed literature review of the recent work in m-commerce payment systems. Section 4 presents a summary of the recent work in the area. Section 5 presents the findings and future scope of research in the area. Finally, Section 6 offers the conclusion.

## II. RESEARCH OBJECTIVES

Following research questions (RQ) have been framed for conduct the review in an organized manner in order to obtain the recent research status in Mobile Payment Security.

RQ1. What are the various proposed models of security?

RQ2. What are the various technologies of Mobile Payment Security?

RQ3. What Security Protocols have been used?

RQ4. What is the future scope of research in Mobile Payment Security Techniques?

## III. METHODOLOGY

To achieve the above mentioned objectives, the author has followed the research methodology portrayed in Figure 2. In the first phase, following Research Repositories are selected to search the required research contents:

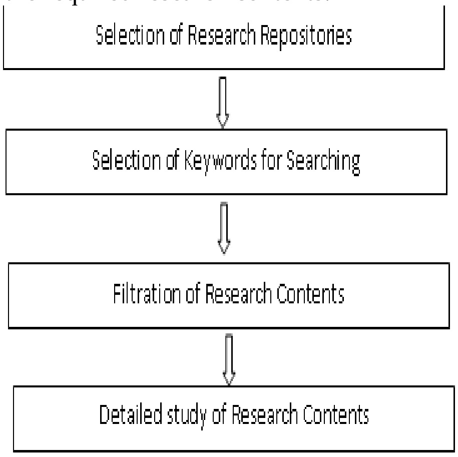
Selection of Research Repositories
Selection of Keywords for Searching
Filtration of Research Contents
Detailed study of Research Contents

**Fig 1: Stepwise Review Process**

- IEEEXplore Digital Library (http://ieeexplore.ieee.org)
- ACM Digital Library (http://portal.acm.org)
- Springer
- Others (Google Scholar, Research Gate, Academia.edu )

In the second stage, various appropriate keywords are used to search the required research contents. As a result, a total of 318 research papers were found. Table 1 enlists the keywords used and their results.

**Table 1: Search Results**

| Database | “M-Commerce payment systems + models” | “M-commerce payment system + security” | M-commerce payment system + technologies” | Total |
|---|---|---|---|---|
| IEEExplore | 12 | 16 | 16 | 44 |
| ACM Digital Library | 02 | 7 | 8 | 17 |
| Springer | 04 | 03 | 03 | 10 |
| Total | *18* | 26 | 27 | 71 |

In the third stage, the authors filtered the search results by going through the abstract of each and every paper appeared in the keyword search results and assessing their suitability for this study. Thereafter, the papers were accepted or rejected based on the specific selection criteria. At the end of reading all the abstracts, following papers were considered into literature.

## IV. RELATED WORK

The authors [5] of this paper proposed a model called SeMoPS (Secure Mobile Payment for Mobile System) based on Wireless Application Protocol. Their model involved six elements namely client, trader, Mobile Network Operator (MNO) which performs the task of processing the client payment apart from playing the role of wireless access provider, bank is the financial institution where the client and merchant accounts are present, Trusted Third Party (TTP) are the organizations that come into picture in case of any disputes and Data Center which performs the function of routing and delivering notifications to addressee and payment processor. Their Model was divided in to five steps: Transferring information, Payment request, payment notice, payment confirmation, Transferring amount. The results show that the model gives reliable and trusted mobile payment services to the customer with no threat about security lapse of private and sensitive information.

A new domain based model was proposed by the authors in [6] with the extension of classical payment model. Their model had provision for considering intermediating entities which had several payment options, payment through smartcards and trusted networks and condition based connectivity of devices. Their model is based on the assumption that all elements can be categorized into separate domains and it permits the authors to consider the mobile security problem as a global issue which is considered as an inter-domain problem. The link between multiple adjoining domains shows a breach of trust between the participating users. This model suggested that global security is an inter-domain problem.

An authentication model was proposed by authors in [7] for third party where they proposed the use of private key cryptography technique to authenticate the mobile client and the merchant to Third Party. Their technique used private key cryptography between Third Party and the merchant as many several sensitive data and information is obvious to be communicated from Third Party to the merchant, and the resource available with merchant terminals are limited. The results show that the proposed protocol model can meet the requirements of minimality, manageability and Single Sign-On. It can avoid large scale of identity theft because the trusted third party doesn’t need to keep the buyers’ important payment information, such as credit/debit card information.

Authors of this paper [8] proposed a Client Centric Model using digital signatures which had provision of recovery of message. The speciality of their model is the presence of an anonymous protocol that used public key. Their model does not permit merchant to hold communication with the acquirer and but the communication among these parties still happen as per the scheme discussed in the proposed model.

A mutual authentication model was proposed by [9] where all the parties involved in the transaction need to prove their identities to each other through authentication with Third Party. They used Private key cryptography as a medium of secure communication among Third Party, merchant and the consumer. The results proved that the proposed model fulfils all the necessary requirements and adhere to the set parameters.

Authors of this paper [10] proposed a Mobile Payment Model based on Wireless Application Protocol where they emphasized on client authentication, trust & relationship, model architecture and the transaction process. This model can be designed to work well with in guided/wired and unguided or wireless networks. It is advantageous in a sense that it provides inter-organizations support and allows interoperability to impose dynamic security.

Authors of this paper [11] proposed a model which they referred to as “SeMoPS model” that ensure secure mobile payment service. In this model the bank acts as the mobile payment handling agency which is associated with the network operator and uses the WAP2.0 protocol which is used for end to end security. SeMoPS model is divided into five steps:

1. Transaction information is sent by the merchant to the mobile client.
2. Mobile client user enters their transaction details in the form of card number, pin etc and this information are sent to the customer bank.
3. The bank verifies the details inputted by mobile client and after successful verification the transaction amount information is sent to the merchant bank.
4. The merchants receive Payment Notice from their bank and then it confirms with the opposite merchant to ensure whether the transaction should continue.
5. The merchant confirms about the transaction and gives a nod to accept the payment. The payment then gets credited to merchant bank account and the transaction is ended.

After successful implementation still the model doesn’t give confirmation whether the payment was successful or not. So he further optimized the model and divides it into seven steps.

1. Transferring information
2. Payment requests
3. Fund freezing
4. Payment notice
5. Payment confirmation
6. Transferring amount/thawing
7. Transferring amount/thawing notice

Authors of this paper [12] proposed a 4iPAY model which had provisions for ubiquity and which is not dependent on any device, location or carrier and which allows payment from mobile devices.

The authors have summarized these recent Papers in Table 2 according to various criteria.

**Table 2: Summary of Recent Papers on Models Proposed for M-commerce Payment System**

| Year/reference | Model proposed | Techniques discussed | Technology used | Protocol used | Results |
|---|---|---|---|---|---|
| (Wei jianping, 2011) | SeMoPS Model | A five step technique was discussed that involved information transmitted, request for payment, notice for payment, confirmation about payment and the amount transferred. | Mobile IP technology<br>3G Technology<br>WLAN Technology | WAP2.0 | The results show that the model gives reliable and trusted mobile payment services to the customer with no threat about security lapse of private and sensitive information. |
| (Roehrs, et al, 2012) | 4iPay | •allows mobile transactions for ubiquitous computing which is not dependent on device, location or carrier | NFC(Near Field Communication) | SOAP (Simple Object Access Protocol), REST (Representational State Transfer), SMS (Simple Message System) and JMS (Java Message Service) | The model proposed was reliable and it also provides more security. |
| (D Suarez et al , 2007) | Domain based Payment Model | Based on three factors: intermediary factor, NSC factor ,connectivity factor. | Wireless mobile networks | TCP/IP | This model provides a global security as an inter domain problem. |
| (M. Song et al, 2007) | Third Party Authentication model for mobile payment. | It used private key cryptography to ensure user authentication also provides credit standing information to the client and the merchant. | Symmetric key cryptograph | KryptoKnight protocol+ X.509 protocol=The new protocol | Ensure no identity theft and proves to be a reliable technique. |

| | | | | | |
|---|---|---|---|---|---|
| (Jesu's Tellez et al 2007) | Client Centric model | Uses Digital Signature and public keys | Digital Signature; public keys | New protocol | Works well without directly contacting acquirer into communication. |
| (M Song et al 2007) | Mutual Authentication model | It used private key cryptography to ensure user authentication also provides credit standing information to the client and the merchant. | Symmetric key cryptography | KryptoKnight protocol | Reliable model. |
| (Jian Meng, Liang Ye, 2008) | WAP based Mobile payment model. | Uses bridge Certificate Authority (CA) authentication to improve the collaboration between the participants. | WAP and Cryptohgraphic algorithms | WAP | This model proves to be good in several aspects and parameters. |
| Jun Liu et al, 2005) | System Model | This model is divided into six elements: customer, merchant, MNO, bank, trusted third party (TTP), DC. MNO | WAP | New Protocol | It presents a new payment and non-repudiation mechanism to improve privacy and the reliability of dispute resolution. It is also cost-efficient. |

## V. RESULTS, FINDINGS AND DISCUSSION

This section provides the analysis of security in m-commerce payment systems. Table 3 summarizes the proposed techniques on two parameters. The critical analysis of m-commerce payment system in the paper has the following findings:

- The findings from the study reveal that majority of the approaches proposed by researchers in recent times are based on cryptography or encryption techniques for ensuring m-commerce transaction security.

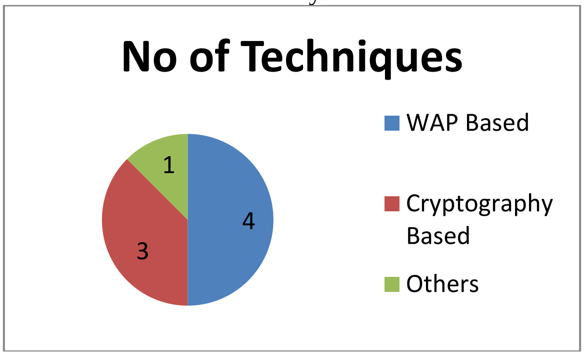

**Figure 2: Techniques Categorization**

- Figure 2 depicts the techniques proposed according to the protocol and type used. The findings state that WAP is becoming the base for all proposed techniques and few of the techniques are using cryptography.
- Most of the models are based on Wireless Access Protocol (WAP), but in some models authors has proposed a new protocol which is an extension to WAP protocols or which deploy WAP in their functioning. Thus it can be said that WAP forms the basis for most models that have been proposed recently.
- All the proposed models have one thing in common: They are ensuring the transaction security without loss of private information which users share on the network during transaction between merchant and consumer.

**Table 3: Summary of Techniques Proposed in Literature**

| Model/ Technique Proposed | Security Achieved(Y/N) | Protocol used(Y/N) |
|---|---|---|
| SeMops | Y | Y |
| 4iPay | Y | Y |
| Domain based Payment Model | Y | Y |
| Third Party Authentication model for mobile payment. | Y | Y |
| Client Centric model | Y | Y |
| Mutual Authentication model | Y | Y |
| WAP based Mobile payment model. | Y | Y |
| System Model | Y | Y |

- As all the models proposed a security between merchant and consumer, still there is scope of research in security between merchant and acquirer. Moreover, the proposed techniques need to be evaluated on other parameters like time taken, reliability and so on.

## VI.CONCLUSION AND FUTURE SCOPE

In this paper, the authors have proposed various models for secure m-commerce payment systems. The various findings under each research question was critically analyzed and presented. Various technologies and protocols have been used in the proposed model has also been analyzed. The findings state that a lot of models and techniques have been proposed in literature but there is a need to evaluate these techniques on various suitable parameters to ensure they are safe and can be used in creating commercial solutions. At last, the future area(s) of research have been suggested.

## REFERENCES

1. Laudon, C. Kenneth and Traver, Carol , E-Commerce, New Delhi: Pearson Education,2010
2. SEI Digital Library [CNSS 2010] Authentication,resources.sei.cmu.edu/asset_files/.../2014_011_001_81821.pdf
3. A. Wadhaval, R. Mehta, A. Gawade, "Mobile Commerce and Related Mobile Security Issues", International Journal of Engineering Trends and Technology (IJETT), Vol 4, Issue 4, 2013,pp 668-672,
4. R. Tandon, S. Mandal, D. Saha, "M-Commerce-Issues and Challenges", In the proceedings of 10th Annual International Conference on High Performance Computing, (HiPC,2003), 2013,Dec 17-20
5. J. Liu, J. Liao, and X. Zhu, "A System Model and Protocol for Mobile Payment", In the Proceedings of International Conference on e-Business Engineering, 2005.
6. D. Suarez1, J. Torres1, M. Carbonell1 and J. Tellez, "A new domain-based payment model for emerging mobile commerce scenarios", In the Proceedings of 18th International Workshop on Database and Expert Systems Applications, IEEE,2007, pp. 713-717.
7. M. Song , X. Hu , J. Li , G Deng, "An Authentication Model Involving Trusted Third Party for M-Commerce" In the Proceedings of the International Conference on the Management of Mobile Business, July 09-11, 2007, pp.53-58.
8. J.T. Isaac, J. S. Cámara, "Anonymous Payment in a Client Centric Model for Digital Ecosystems", In the *Proceedings of IEEE International Digital Ecosystems and Technologies (IEEE DEST)*, 2007.
9. M. Song, J. Li, X. Wu, "A Mutual Authentication Model between Merchant and Consumer in M-Commerce" In the proceedings of *International Conference on Innovative Computing Information and Control*,2007, pp. 489-489.
10. J. Meng, L. Ye, "Secure Mobile Payment Model Based on WAP", In the *Proceedings of 4th IEEE International Conference on Wireless Communications Networking and Mobile Computing*, 2008 ,pp. 1-4..

## AUTHORS PROFILE

**Ms. Deepika Dhamija**, pursued Master of Computer Applications from Kurukshetra University Kurukshetra and is presently working as an Assistant professor at Amity University Haryana. She is a Ph.D. research Scholar at Computer Science & Engineering Department at Sunrise University Alwar, Rajasthan. During her teaching experience of almost ten years, she has published various research papers in International and Referred Journals. She has also presented research articles at various national and international conferences. Her areas of interest include M-commerce, System Security issues, Cloud Computing and Management Information System.

**Dr.Anu Bharti**, is Dean of Engineering in Sunrise University ,Alwar, Rajasthan.She has published various research papers in International and Refereed Journals.