CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

M-commerce service is launched as an offshoot of the wireless communication technology. With an eye on assuring a superb degree of security, simultaneously maintaining the ease of ubiquity is a puzzled realism in the domain of M-commerce applications, putting insurmountable roadblocks in its pathway of extensive employment. Even if satisfactorily validated at the beginning of a transaction series, the messages may likely be interrupted, especially within a compromised gadget before sending the message or within the network. The vital stipulation for safety in M-commerce services is that both the user and his/her mobile device involved in a transaction must be authentic. Nevertheless, a large majority of the mobile networks employ pre-stored password or PIN to restrict access. This chapter is dedicated to review the issues related to problems encountered in the security of M-commerce and which has influenced to carry out the work presented in this thesis.

2.2 RELATED WORKS

It is necessary to do a complete survey/study of the existing M-commerce, to understand the requirements of a reliable M-commerce system. In this context, the survey has been done related to safety and authentication issues, reliability, user satisfaction, sequential pattern, protocol in M-commerce system and those ideas are presented in this section. This
kind of surveys helped in many ways in this work to frame and construct the forthcoming chapters.

### 2.2.1 Safety Issues in M-commerce

M-commerce offers a thrilling set of new capacities which the service providers can control for the purpose of enhancing their income base simultaneously inviting novel services that lead to the enhancement of the end-user experience. With these novel opportunities, the risk of fresh safety challenge crops up which have to be tackled carefully. Cai Yigang et al (2004) discussed the safety issues and particularly dealt with service and subscriber authorizations in improved prepaid executions for M-commerce. These products characteristically furnished a renovated rating engine and a vastly configurable feature set for service and content charging in wireless networks. The solution architectures and a debate of authorization standards were also offered.

The prospect of making the Internet accessible using mobile devices has created a significant opportunity for electronic commerce. However, certain lacunas prevent a large-scale use of M-commerce applications. In this regard, safety and convenience of use remain as indispensable stipulations. The employment of brokerage systems represents an enthralling solution to speed up the data delivery to the users. Further, the brokers are competent to utilize the mobile agents so as to effectively and conveniently carry out the search and reclamation of commercial data on the Internet. Though the mobile agent technique is a very appropriate option for the M-commerce domain, there is a multitude of safety challenges that block its use. Especially, a significant feature that has to be tackled for the M-commerce setting is the mobile agent safety from manipulation ambushes carried out by the malevolent hosts. Oscar Esparza et al (2006) elegantly proposed a novel system to attain the related safety. They dwelt deeply on the
method in which software watermarking methods could be used in the mobile agent to identify the manipulation ambushes, and the manner in which the broker was able to thwart the malevolent hosts. When an M-commerce site was chosen by the user, an end-to-end safe transaction was put in place, which employs various protocols, from an easy and safe TLS channel to forward a credit card number till a classy payment protocol. However, Public Key Certificates (PKCs) are needed for these protocols. It was to be emphasized that the certificate management was a profound procedure and that clients in the brokerage domain faced resource-crunch. There the excellent option was for the clients to delegate the relative duty to the broker. It was noted that the broker was a Trusted Third Party (TTP) and had sufficient resources. So, the broker was suitable for storing and managing PKCs. The latter part of their document tackled this dilemma, with special emphasis on the certificate status management that was the most intricate function of the certificate management.

With the onset of wireless communication and internet protocol, several techniques have been designed to furnish the mobile phone user with the wireless internet service. Security supporting wireless internet has to be ensured at an identical level of the wired security. But PKI (Public Key Infrastructure) which was employed for the safety of E-commerce in wired internet was not viable for the mobile phone in view of the basic constraints of accomplishment like the reduced memory and less dominant CPU. Hence, there is a need of designing a wireless PKI (WPKI) which offers an identical level of safety as that of the wired PKI supporting the mobile phone. Yong Lee et al (2007) valiantly launched the wireless PKI technology and demonstrated the performance outcome of the innovative wireless PKI technology on the newest mobile phone. They were able to reduce the data dimensions processed in the mobile phone, and optimize protocols for the certificate management and authentication between mobile phone and server.
The outcome in the decrease module sizes was sufficient to install in the mobile phone. There, their innovative WPKI technology illustrated that security was in an identical level with that of the wired PKI and the entire PKI processes were efficiently processed in the mobile phone.

Hakjae Kim et al (2009) launched a novel user authentication for the Internet service which was activated by using the driver's fingerprint, instead of typing his/her password. As the driver's fingerprint needed to be safeguarded, and the size of the fingerprint data was exceedingly bigger than that of a typical password, they required a diverse user authentication protocol for the telematics environment. In other words, along with the compliance of standard X9.84 protocol to safeguard the fingerprint information transmitted, they utilized the watermarking method to reduce the confidentiality challenge, and launched a safe and effective protocol between Access Points (APs) taking into account the possible hand-off during the verification in the mobile telematics scenario. By the test evaluation of the novel protocol, it was established that the fingerprint-based user authentication could be performed in real-time in the telematics atmosphere.

Chin-Chen Chang et al (2010) proposed that a large number of mobile users were permitted to utilize the wireless networks, as universal access was exceedingly encouraged. A there was no single, reliable authentication server; it had become a severe issue to safeguard the inter-domain safety, which enabled the users to travel into foreign domains. Therefore, an authentication mechanism was the need of the hour to be used between mobile users and foreign servers, and an authentic key also was also essential to support safe communications in wireless networks. Moreover, the preservation of the secrecy of users was a vital safety need including the data regarding the customer behavior. The modern research invested its total attention on the related challenges and also offered definitions and certain
constructions. Significantly, Tang and Wu launched an effective mobile authentication scheme, which they named as “Efficient Mobilization Authentication Scheme” (EMAS), which sparkled with computational and communication effectiveness surpassing those of the peer mobile authentication schemes. However, it was unfortunate that Tang and Wu’s scheme could not satisfy the vital safety needs. Hence, with a view to designing a further satisfactory mobile authentication technique, a novel self-verified mobile authentication scheme is launched, which is endowed with an innovative architecture. The study concluded to furnish superior computation efficacy and storage effectiveness; the innovative scheme doesn't need any long-term secret keys on the servers.

A host of investigations has been carried out progress with advantage regarding meeting the critical safety needs of M-Commerce, involving the identification and resolution of a large majority of the probable errors. Nevertheless, modern investigations have emphasized the fact that a specific attack, termed as the wormhole attack, is capable of causing irreparable damage to the routing protocol. This susceptibility is present in a wireless system, and it is also likely to exist in ad hoc commerce systems. Though several efforts have been made to face the wormhole attacks in the domain of wireless communications, the offered solutions seem to be insufficient, requiring further renovation. For instance, the Ariadne-based techniques have been plagued with fresh insider ambushes, thought till date susceptibility has not yet been successfully tackled. Also, the relative solutions have not been adapted for a Mobile commerce scenario. Hao Ting Pai et al (2011) were able to locate a potential new threat from wormhole ambushes in an ad hoc M-commerce scenario and came out with a novel technique for addressing such kind of ambushes in such a way that it was not affected by the fresh challenges encountered by the Ariadne and endairA. In accordance with the cryptographic theory, in their document they discussed
that the novel technique was able to overwhelm the wormhole ambushes arising from both the exterior involving non-approved and non-legitimate identities, and the interior involving the approved and legitimate identities. The vital traits of their solution were: (1) in the routing request task, grave computation could be jeopardized among dominant servers; and (2) in the routing reply function, only some source node decrypted all the cipher text communicated by intermediate nodes and it is not obligatory every intermediate node to carry out the cryptographic computations.

Daojing He et al (2011) proposed that flawless handover over multiple access points was extremely attractive to mobile nodes, though providing for the safety and efficacy of the relative procedure was daunting. In their document, they illustrated that preceding handover validation schemes incurred extremely elevated communication and computation expenses, and were prone to several safety ambushes. Moreover, an innovative handover validation protocol called PairHand was elegantly launched, which employed the pairing-based cryptography to safeguard the handover process and to realize superb efficiency. Moreover, an effective batch signature verification scheme was also integrated into the PairHand. Test outcomes employing the implementation of the technique on laptop PCs illustrated that PairHand was viable in authentic applications.

Alomair et al (2012) proposed that with the present-day sophisticated technology, several applications invariably depended on the existence of minor devices that were able to convey data and form communication networks. In a large majority of such applications, the privacy and honesty of the conveyed messages assumed supreme significance. In this document, they launched two innovative methods for validating short encrypted messages that were directed to satisfy various needs of mobile and pervasive applications. Benefiting from the fact that the message to be
validated had to be compulsorily encrypted, they introduced provably safe validation codes that were found to be more effective than any other message validation code in the literature. The vital concept behind the innovative methods was to use the safety that the encryption algorithm was able to provide to device further effective validation techniques, quite different from employing the standalone validation primitives.

The group-buying technology has emerged as an appealing commerce service, equipped with the merits of discount and easiness. However, there is a host of various deficiencies the modern group-buying systems. The most pertinent one is the lack of safety concerns resulting in the exposure of the confidentiality of the participants concerned. Further, the buyers have to effect payment to the initiator in advance. In the absence of a reliable third party to oversee the purchase, the initiator may disappear after pocketing the money. Jung-San Lee et al (2013) took the trouble of alleviating the risk of the related deficiencies by launching a novel system envisaging a group-buying server to safeguard and supervise the transaction. As the server functioned just as a mediator, it was competent to assist the buyer and vendor to bargain with each other using a safe channel. Mutual validation between the customer and merchant was ensured under the BAN, logic model. Especially, they utilized the Bloom filter and XOR operation to decrease the dimension of the transaction table and the computational expenses.

Of late, the necessity for an added safety for amazing private and business data or accessing corporate networks on mobile devices is growing at an exponential rate, and one of the probable solutions is to utilize novel biometric authentication method. Klonovs et al (2013) naively offered the design of a mobile biometric authentication system in accordance with the electroencephalogram (EEG) recordings together with previously established techniques like the facial detection and near field communication (NFC). The
ultimate aim of the work was to engulf the gap between mobile Web techniques and wireless EEG gadgets and to design an authentication method and a viable application. Hence, they assessed the pertinent literature, carried out various EEG measurement tests, and conducted debates regarding the process and outcomes with the specialists in the EEG and digital signal processing (DSP) domains. In line with the outcomes, they were able to configure and launch a mobile prototype system equipped with skills to validate the users on the basis of distinctiveness of their brain waves.

Ortiz Yepes et al (2014) designed a novel mobile-device-oriented techniques intended to offer strong validation and transaction safety. In their document, they took into consideration the e-Banking application environment and advocated that the idea of employed a reliable companion device can be ported to the mobile domain. Reliable companion tools include the recognized and proven method in the PC (personal computer) scenario to safeguard the transactions. Several options for the communication between mobile and companion devices were the subject matter of debate and were assessed concerning the technical viability, usability, and expenditure. As a result, the audio communication across the 3.5-mm audio jack—also called the tip-ring-ring-sleeve, or TRRS connector,—was decided to be wholly suitable. A proof-of-concept companion device was launched for performing binary frequency shift keying across this interface and outcomes from a field study carried out with the this device went on establish the viability of the innovative solution.

2.2.2 M-commerce Reliability

Reliability is a characteristic of any commerce transactions that reliably performs according to its configurations. It has been one of three related attributes that must be considered when making, buying, or using a mobile product or component. It is essential to implement several networking
requirements in the mobile and wireless networks to ensure the reliability and efficiency of M-commerce application.

Liao et al (2005) proficiently offered an innovative technique for learning Bayesian networks from functional dependencies (FD) and third normal form (3NF) tables in relational databases. The proposal technique established a linkage between the concept of relational databases and probabilistic reasoning models, which was enthusing and functional particularly when the data were found deficient and imprecise. The efficiency and viability of the ground-breaking approach were illustrated by its execution in a Mobile commerce system.

In the distributed mobile systems, communication expenses and disconnections were the supreme concerns. Manghui Tu et al (2006) took the trouble to tackle the replica placement challenges to realize augmented efficiency for systems supporting mobile transactions. They invested their attention on addressing the related data objects and disconnections. Habitually, requests and transactions issued by mobile clients might access multiple data objects and had to be considered jointly in terms of replica allocation. They discussed the replication cost model for related data objects and illustrated that the challenge of locating an optimal solution was NP. Moreover, they adopted the replication cost model for disconnections. A heuristic "expansion-shrinking" technique was designed for making effective replica placement decisions. The algorithm was able to attain near optimal solutions for the related data model and accomplished considerable performance advantages when disconnection was taken into account.

Though there has been a feast of discussions on transactions in Mobile E-commerce (M-commerce), no significant consideration has been paid for distributed transactional properties of the computations enabling M-commerce. Jari Veijalaine et al (2006) elegantly offered an evaluation for M-commerce.
commerce transactions, a graph-based transaction model, and Transaction Manager (TM) architecture for a wireless application which safeguarded the M-commerce workflows preventing the occurrence of the communication link, application, or terminal crash. The modules, application interface, and log structure performance of this TM for the location-based application were offered. In addition, they deliberated on the other options to design an innovative TM which as a whole can be labelled as the Ontological Transaction Monitor, which took the responsibility for closely watching the constraints concerned with safety and secrecy.

In the up-and-coming wireless Internet scenario involving M-commerce and other mobile applications, a zooming number of users are getting interested in the adoption of mobile transactions. These transactions have many different needs, some requiring a considerable amount of network resources and bounded delays. One of countless distinctive traits of transactions involving a financial value is the criticality of its conclusion. The distinctive needs of mobile transactions entail the launching of novel metrics for quality-of-service. In the past, a large majority of the quality-of-service research in wireless networks were concentrated on call or connection-level QoS. Ahluwalia et al (2007) came out with a novel structure to support QoS needs of mobile transactions by resource allocation at the connection level, transaction level, and a blend of the connection and transaction levels. To evaluate the QoS efficiency of mobile transactions, two metrics such as the transaction completion probability and transaction response time, were launched. Replication and analytical techniques were employed for evaluating diverse metrics for transaction efficiency under fluctuating network and traffic scenarios. The outcomes illustrated that the balanced transaction and connection level resource allocation were able to enhance the prospect of transactions completion and resource exploitation. Therefore, augmentation
resulted in marginally enhanced processing expenses, which depended on the group dimension and number of transactions during a connection.

Swift growth in software systems, wireless networks, and embedded devices resulted in the advancement of a pervasive and mobile cyberspace which offered an infrastructure for anywhere/anytime service provisioning in several regions like the engineering, commerce, education, and entertainment. With the result, users were empowered to move freely between geographical areas and to incessantly access data and conduct online transactions. Nevertheless, this kind of extreme mobility might result in efficiency and dependability challenges while performing the transactions. For instance, the lack of enough bandwidth could lead to the collapse of transactions when users shift from one area (cell) to another. Younas et al (2012) innovatively launched a context-aware transaction model which dynamically adjusted to the users' requirement and implementation scenarios. Therefore, they envisaged a mobility management scheme which facilitated flawless connectivity and consistent execution of context-aware transactions in the course of the mobility of users. Their innovative technique was envisioned and launched using a blend of diverse queuing models. They also carried out several tests that showed without an iota of doubt that the novel scheme was able to optimize the mobility management procedure and enhance the throughput of context-aware transactions.

Alain Yee-Loong Chong (2013) conducted investigation of the predictors of M-commerce adoption by enlarging the Unified Theory of Acceptance and Use of Technology (UTAUT) model, which integrated supplementary constructs like the apparent value, trust, apparent enjoyment and individual innovativeness. A non-linear, non-compensatory model was designed to comprehend the predictors of M-commerce adoptions. Neural network analysis was employed to forecast M-commerce adoption, and the
model was assessed and analysed with the outcomes from regression evaluation. The neural network model was found to outsmart the regression model in adoption accuracy, and encapsulated the non-linear associations between predictors like the apparent value, trust, apparent enjoyment, individual innovativeness, user's demographic profiles such as the age, gender and educational level, effort anticipation, performance anticipation, social power and enabled conditions with the M-commerce adoption. In the document, the neural network was performed to furnish added awareness of the M-commerce adoption decisions by the non-linear, non-compensatory model. The UTAUT technique was also expanded to investigate the consumer data systems such as the M-commerce.

2.2.3 M-commerce User Satisfaction

A host of tools for evaluating the user-perceived system quality and user data satisfaction were designed in the backdrop of mainframe, PC and wire-based technologies of a departed era. With the explosion of wireless technologies, users started using the interfacing and interacting with Mobile commerce systems in a spectacular way. It was, therefore, essential to launch novel gadgets and scales, directly intended for these novel interfaces and applications. Client delight is habitually accredited as one of the valuable proxy measures of the system efficiency. Yi-Shun Wang et al (2007) took great pains to address the concern for an efficient M-commerce system design by way of the conceptualization and measurement of an M-commerce user satisfaction (MCUS) construct. In their document, they innovatively launched and detailed the construct of MCUS, furnished practical authentication of the construct and its fundamental dimensionality. They also designed a standardized tool with attractive psychometric traits for evaluating the MCUS, and investigated the measure's conceptual and realistic application.
Lu et al (2011), gave an extensive variety of promising applications, investigation on M-commerce that attracted the zooming enthusiasm of both the industrial magnates and the academic cream. Out of them, one of the liveliest subjects related to the mining and forecasting of the Mobile commerce behaviour of the clients as their movements and purchase deals. In this document, they launched an innovative structure known as the Mobile Commerce Explorer (MCE), for mining and forecasting of mobile users' movements and purchase deals against the backdrop of Mobile commerce. The MCE structure comprised three vital segments as detailed below.

i. Similarity Inference Model (SIM) for evaluating the resemblances among stores and items, which were the two fundamental Mobile commerce entities taken into account in this document.

ii. Personal Mobile Commerce Pattern Mine (PMCP-Mine) algorithm for the effective discovery of mobile users' Personal Mobile Commerce Patterns (PMCPs)

iii. Mobile Commerce Behaviour Predictor (MCBP) for forecasting potential mobile user behaviours. As far as our knowledge goes, this is the preliminary work that enables the mining and forecast of mobile users' commerce behaviours with a view for recommending stores and items unfamiliar to the user in the past.

The progress in the wireless communications brought about a zooming number of people employing the mobile devices, and speeded up the advancement of Mobile commerce (M-commerce). Alain Yee-Loong Chonge et al (2012) explored the factors that went a long way in forecasting the
consumer plan to adopt M-commerce in Malaysia and China. The study enlarged the traditional technology acceptance model (TAM) and the diffusion of innovation (DOI) model, and incorporated supplementary variables like the trust, cost, social power, diversity of services, and control variables like the age, educational level, and gender of consumers. By making a comparison of consumers from both Malaysia and China, the related investigation was able to configure a forecast model based on two diverse cultural settings. Data was gathered from 172 Malaysian consumers and 222 Chinese consumers, and hierarchical regression evaluation was used to evaluate the research model. The convincing outcomes illustrated the fact that the age, trust, cost, social power, and diversity of services were competent to forecast the Malaysian consumer decisions to adopt M-commerce. In this regard, trust, cost, and social power could be employed to forecast Chinese consumer decisions to adopt M-commerce. The captioned investigation emphasized the requirement for extending the time-tested TAM and DOI models while investigation technology like M-commerce. The outcomes from the relative investigation would be very fruitful for telecommunication and M-commerce companies designing their marketing strategies.

2.2.4 Mobile Sequential Pattern

Mobile sequential patterns are applied for planning M-commerce environments and also for analysing and managing online shopping websites. Ching-Huang Yun et al (2007) got name and fame for exploring a data mining capability for a Mobile commerce scenario. For efficiently reflecting the customer usage models in the Mobile commerce atmosphere, they elegantly launched a mining model, termed as the mining mobile sequential patterns, which took into account both the moving patterns and purchase patterns of clients. They went to design three algorithms such as the TJLS, TJPT, and TJPF algorithms for deciding the frequent sequential patterns, which were
called large sequential patterns in their document, from the mobile transaction sequences. The TJLS algorithm was envisioned in a backdrop of the idea of association rules and was employed as the fundamental method. Whereas the TJPT algorithm was designed by integrating the notions of the association rules and path traversal models which resulted in efficiency enhancement using the path trimming. The TJPF, in turn, was designed by exploiting the pattern family method which was envisaged to utilize the association between the moving and purchase behaviours, and thus was competent to produce huge large sequential patterns very effectively. A replication technique for the Mobile commerce scenario was brought to light, and a synthetic workload was created for the efficiency evaluation. In mining the mobile sequential patterns, the test outcomes illustrated the fact that the TJPF algorithm incredibly outsmarts its peers in the performance of excellence and memory saving, underscoring the efficacy of the pattern family method introduced in their document. The captivating outcomes made it crystal clear that by taking into account the moving and purchase patterns, it was feasible to configure a superior model for a Mobile commerce system which would be competent enough to utilize the innate association between these two vital factors for the proficient mining of mobile sequential patterns.

Ting-Yi Chang et al (2012) proposed a sequential pattern technique (as a user authentication technique) for touch screen handheld mobile devices. A large majority of the user authentication technique for these mobile devices employed PIN-based (Personal Identification Number) authentication, as they did not use a standard QWERTY keyboard for easily entering text-based passwords. Nevertheless, PINs offered a small password space size, which was susceptible to ambushes. Several investigations had utilized the KDA (Keystroke Dynamic-based Authentication) system, which was dependent on keystroke time traits to improve the safety of PIN-based authentication. However, unlike the text-based password KDA techniques in QWERTY
keyboards, various keypad sizes or layouts of mobile devices affected the PIN-based KDA system utility. In their document, they launched a novel graphical-based password KDA system for touch screen handheld mobile devices. The graphical password broadened the password space size and supported the KDA utility in touch screen handheld mobile devices. Moreover, the document envisaged a pressure feature, which was simple to use in touch screen handheld mobile devices and was employed in the novel system. The test outcomes illustrated that (1) EER was 12.2% in the graphical-based password KDA novel scheme system. In comparison with connected schemes in mobile devices, this efficiently promoted the KDA system utility; (2) EER was decreased to 6.9% when the pressure feature was employed in the innovative system. The precision of authenticating keystroke time and pressure features was not affected by incompatible keypads as the graphical passwords were entered by means of an matching size such as (50 mm × 60 mm) human–computer interface for satisfying the lowest touch screen size and a GUI of this size was exhibited on all mobile devices.

2.2.5 M-commerce Protocol

Presently most of the mobile protocols are very similar to each other, being client-server based, enabling a continuously increasing amount of services to be provided to the users. Also these protocols are introducing some challenges to the adoption of widespread M-commerce since it is more difficult to get a certain critical mass of subscribers to use a universal technology to enable frictionless service providing. So there is a need for the development of a number of M-commerce protocols, which ensures confidentiality, integrity, atomicity and fair exchange. However most of the mobile protocols are very similar to each other, being client-server based, enabling a continuously increasing amount of services to be provided to the users. These protocols are introducing some challenges to the adoption of
widespread M-commerce since it is more difficult to get a certain critical mass of subscribers to use a universal technology to enable frictionless service providing. The future will show which protocol is going to deliver the strongest commercial value at any point in time and will be supported by the largest number of attractive applications.

Hui Chen et al (2007) elegantly launched the MAGICS, a mobile agent-based system for supporting business-to-consumer electronic commerce (E-commerce) or Mobile commerce (M-commerce) applications. For the purpose of using the system, consumers had to furnish all their buying needs to a proxy/agent server by means of a Web browser or a wireless application protocol (WAP) terminal. After obtaining the needs, mobile agents were created to perform the functions for the consumers including receiving offers from merchants, assessing offers, and even finalizing purchases. In the case of Mobile commerce, consumers could create a mobile agent to carry out an investigation and assessment search and evaluation in the digital market space prior to affecting a purchase in the physical marketplace. So as to select an offer that best suited the consumer's needs(s); a mathematical model was presented for estimating the multiple decision factors. To evaluate the fundamental functions of the mobile agent-based Internet commerce system (MAGICS), a prototype system was also configured. To reduce the average expense of a product (including the cost of sending agents), an analytical model was designed which could decide the number of agents to be sent to analyze the prices. Four various price distributions and certain authentic data were assessed depending upon the model. The assessment furnished valuable insights into the design of mobile agent-based shopping applications particularly for M-commerce, and generally for E-commerce.

For safe communications in public network scenarios, several three-party authenticated key exchange (3PAKE) protocols were launched to
usher in the utmost transaction secrecy and effectiveness. Jen-Ho Yang et al (2009) was instrumental in launching a proficient three-party authenticated key exchange protocol in accordance with the elliptic curve cryptography for Mobile-commerce scenarios. As the elliptic curve cryptography was deployed, the innovative 3PAKE protocol yielded trivial computation expenditure and light communication loads.

Mobile scenarios boomingly need the distributed atomic transactions to support the mounting variety of financial, gaming, social networking, and several other applications. The basic mobile infrastructure is growing accordingly with exceedingly various wired and wireless elements and also with escalating exposure to an assortment of functional perturbations at the mobile elements and communication levels. Therefore, the problem lies not only in offering effective non-blocking mobile commit (as a vital base for the steady mobile transactions) but also in furnishing effectively perturbation-resilient atomic commit in the diverse mobile space. The role of this study was to design a perturbation-resilient mobile commit protocol that effectively furnishes and maintains strict atomicity for transactional applications. The protocol does away with the requirement for access to the dominant communication/computation segments of the nervous infrastructure during transaction implementation. Nevertheless, when a wired network is accessed, it adjusts itself to exploit the following; 1) it enhances the resilience to network perturbations realizing superior commit rates, and 2) decreases the wireless message cost and the blocking of transaction participants resulting in the superior transactions throughput. On the contrary, the modern solutions are generally adapted either for 1) infrastructure-based mobile scenarios or 2) infrastructure-less ad hoc networks. Ayari et al (2012) proposed that the perturbation-resilient generalized mobile transaction commit (GMTC)
protocol which characterized the debut atomic commit protocol for hybrid mobile scenarios which 1) takes full benefit of accessing infrastructures, by selecting consistent infrastructure nodes for organization of transactions and for replication of commit data of mobile participants to tackle network disconnections, and 2) offers best-effort outcomes with respect to transaction commit rate, message complexity, and commit/abort decision time (latency). The protocol performance simulations (covering transaction commit rate, message complexity, and commit/abort decision time) illustrated the efficiency of the designed protocol in the generalized mobile scenarios.

Maria De Marsico et al (2014) proposed safe protocols for access and validation on mobile platforms. Mounting aptitude of mobile devices to store and exchange sensitive data evinced greater enthusiasm in utilizing their vulnerabilities, and the conflicting necessity to safeguard the users and their data by means of safe protocols for access and identification on mobile platforms. Face and iris recognition were particularly appealing, as they are adequately dependable, and only needed the webcam usually equipping the involved devices. On the other hand, the optional use of fingerprints needed a devoted sensor. Further, certain types of biometrics were used for purposes which went beyond their security. Ambient intelligence services bound to the detection of a user, in addition to social applications, like the automatic photo tagging on social network were able to employ considerably the face recognition. In their document, they envisaged the FIRME (Face and Iris Recognition for Mobile Engagement) as a biometric application based on a multimodal detection of face and iris, which was meant to be implanted in mobile devices. Both design and performance of FIRME depended on a modular architecture, whose workflow consisted of separate and replaceable packages. The starting one took care of the image acquirement. After this,
various branches carry out recognition, segmentation, feature extraction, and matching for face and iris separately. In the case of face, an anti-spoofing measure was also carried out after segmentation. At last, outcomes from the two branches are combined. With a view to tackle the security-critical applications, FIRME was able to carry out uninterrupted re-identification and excellent sample choice. Moreover, to tackle the probable limited resources of mobile devices, all algorithms were optimized to be low-demanding and computation-light.

2.2.6 M-commerce Authentication Issues

Logging-in to an M-commerce application or website from a mobile device and typing robust passwords for authentication is a cumbersome chore. Consumers of today have tons of passwords, each consisting of a series of upper and lowercase letters, alphanumeric character and special symbols. This traditional approach to authentication is a daunting task and nearly impossible on mobile devices as user struggle to enter their clunky passwords by toggling between multiple tiny, soft keypads. In a recent survey of smartphone users, the majority (60%) said they wish there were an easier form of authentication for mobile apps (Curtis Staker 2011). The charm of Mobile commerce is the ability to complete transactions quickly. But as long as text passwords remain the method for logging in or authenticating transactions, the ease of use promised by mobile commerce falls flat.

Muhammad Khurram Khan et al (2008) got worldwide acclaim for launching an effective and realistic chaotic hash-based fingerprint biometric remote user authentication technique on mobile devices such as the cell phone and PDA. The innovative technique was entirely dependent on the new family of one-way collision-free chaotic hash functions, which were more effective
than the modular exponentiation-based validation techniques such as the RSA. The innovative technique represented a two-factor validation mechanism, and a user was expected to identify him with something he had full knowledge on such as a password and something which represented him such as the fingerprint biometric. The safety evaluation also illustrated the fact that the innovative method furnished safe, vigorous, and dependable remote validation of mobile users over an unprotected network. Further, the computational expenses and the efficacy of the anticipated technique where the appeal for the realistic performance in the authentic scenarios.

Qian Tao et al (2010) were instrumental in bringing to the limelight a safe, vigorous, and cost-effective biometric authentication technique on the personal mobile device for the personal network. The system comprised the following five important modules such as the face detection, face registration, illumination normalization, face authentication and the data synthesis. In respect of the intricate face validation task on the devices with scant resources, the thrust was fundamentally on the consistency and viability of the mechanism. Both conceptual and realistic considerations were taken into account. The ultimate system was capable of realizing an equal error rate of 2% under demanding testing protocols. The trivial hardware and software expenses made the system well suitable to a mammoth variety of safety applications.

Dong-Ju Kim et al (2010) launched an innovative recognition technique based on multiple frame images which were performed on the mobile devices. The ultimate objective was to augment the precision of detection and to scale down the computational intricacy using manifold trials, which indicated that multiple frame images are, was used during the detection process. Out of several sequential frame images, a satisfactory subject, such as the teeth image, was shortlisted by the subject selection module that was
performed by the differential image entropy. The shortlisted subject was thereafter used as a biometric trait of conventional recognition algorithms including PCA, LDA, and EHMM. The efficiency analysis of the innovative technique is carried out with the help of two teeth databases created by a mobile device. The captivating test outcomes proved that innovative technique ushered in augmented detection precision of around 3.6–4.8% and glistened from inferior computational intricacy vis-a-vis the conventional biometric techniques.

Guerra-Casanova et al (2011) focused on the assessment of a biometric method depending on the efficiency of an identifying gesture by catching hold of a telephone with an entrenched accelerometer in his/her hand. The acceleration signals received when the users carried out gestures were evaluated using a mathematical method by the comprehensive sequence alignment. They also proposed eight diverse scores and evaluated with a view to quantify the divergences between gestures, achieving an optimal EER outcome of 3.42% when scrutinizing a arbitrary set of 40 users of a database constituting 80 users with genuine attempts of distortion. Also, a temporal assessment of the technique was offered resulting in the necessity to update the template to harmonize the manner in which users changed their mode of execution of identifying gesture over a period. Six updating techniques were evaluated within a database of 22 users recurring their identifying gesture in 20 sessions over a period of 4 months, proving that the if the template was updated a number of times, a superior and further consistent execution was offered by the technique.

Fuglerud et al (2011) offered a safe and accessible multimodal authentication technique to log in to an Internet banking service. It employed a one-time-password (OTP) client established on a mobile phone which substituted the enthusiastic OTP generators. The client was able to offer both
visual and auditory output, which was dependent on an application authorised for safe log-in to sensitive online services. It permitted usage by people whose functional deficiencies severely affected their capacity to deploy the modern solutions. They also discussed the implications for growth and made various proposals for devising functional and accessible security applications and solutions.

The zooming growth of the Internet and the wide use of mobile phones have enhanced the demand for mobile devices in Internet auctions. This trend is functioning as an inducement to design an auction model for mobile-based setting. Of late, Kuo-Hsuan Huang launched a mobile auction agent model (MoAAM), which allowed the bidders to participate in online auctions by means of a mobile agent. He employed modular exponentiation function in his novel technique. Therefore, the processing duration for key creation, bidding, and verification became protracted. It was proposed to supplement the notion of Elliptic Curve Cryptosystem (ECC) with the MoAAM, as the ECC incurs only trivial computation amount and small key size, which are intended to enhance the speed in creating the keys, bidding, and authentication. As regards the decrease of computation load on mobile devices and auction manager server, the innovative technique is well-geared to make online auction system further effective and well-adapted for employment. Yu-Fang Chung et al (2011) employed the English auction protocol as the key auction protocol, which contains four entities such as the Registration Manager (RM), Agent House (AH), Auction House (AUH), and Bidders (B). The Registration Manager discharges the function of registering and authenticating the Bidder identity. The Agent House controls the agents and allocates the public transaction keys to Bidders. The Auction House offers a location for auction and preserves all the essential functions for an effective online auction. The bidders represent the buyers who wish to buy the
items at the auction. This innovative technique satisfies all the stipulations of an online auction protocol in terms of anonymity, traceability, no framing, unforgetability, non-repudiation, fairness, public verifiability, unlinkability among several auction rounds, linkability within a single auction round, efficiency of bidding, one-time registration, and simple revocation.

Zheng et al (2012) proposed that it was significant, for the safety of satellite mobile communication networks to devise an effective access authentication procedure. Accordingly, they elegantly launched a two-way access authentication technique among mobile users, gateways and the Network Control Centre (NCC). The novel technique passed through four different phases such as the registration and management of the mobile user, mobile authentication and mobile authentication update. Also, the Syverson-van Oorschot (SVO) logic was also brought in to enable the authentication technique to authenticate the safety. The innovative method brought to light the validation role of the gateways and reduced the validation calculation load of the NCC. The ground-breaking scheme was competent to thwart any ambushes encompassing the identity spoofing, meddling, replay and so on. The veracity of the communication data was also safeguarded, thereby beefing up the safety of the satellite mobile communication networks. The novel approach was performed on the developed satellite mobile communication simulation platform. The cheering replication outcomes vouchsafed the fact that the authentic expenditure for the audio service and video service were significantly low. Further, the novel technique was capable of maintaining the quality of service (QoS) of the satellite mobile communication.

An effective mobility management system is one of the vital problems of ubiquitous computing. Of late, the IETF NETLMM working
group launched the Proxy Mobile IPv6 (PMIPv6), a network-based localized mobility management protocol to support mobility management without involving the mobile nodes (MNs) in any mobility-related signalling. However, PMIPv6 is plagued with severe packet losses and long authentication latency in the course of handover. To tackle the challenges, Ming-Chin Chuang et al. (2013), elegantly launched a safe authentication mechanism and swift handover scheme known as SF-PMIPv6 for PMIPv6 networks, which ensured tiny handover latency, backed the local authentication processes and found appropriate solution to the packet loss issue, and successfully tackled the out-of-sequence packets. Besides, the SF-PMIPv6 was found to be a vigorous authentication technique that blocked several ambushes. The replication outcomes also established that it was competent find a superior solution vis-a-vis peer techniques.

Castro et al. (2013) introduced the Runtime Adaptive Multi-factor authentication Environment (RAMEN) which represented a client and server-side framework. It offered multi-factor authentication policy enforcement for mobile devices running iOS® and Android®. On the part of client, RAMEN employed a security manager which was able to intercept network calls and send them for safe validation to a server-side proxy, which consisted of a vibrant policy engine configured to select between various validations schemes depending on the mobile scenario. The RAMEN represented an extensible framework which had interfaces to plug in variation validation techniques. The policy model and performance of RAMEN were elaborately dealt with. The significance of RAMEN was demonstrated to developers by means an implementation of location-aware security policies which was established to impose safety zones thereby reducing or increasing the safety needs for diverse applications.
Jianfeng Ren et al (2013) offered a natural and non-intrusive way to safeguard the mobile devices, such as a complete and fully automated face verification system. It contained three sub-systems like the face detection, alignment and verification. The innovative subspace face/eye detector was able to locate the eyes very accurately when compared with the Adaboost face/eye detector. By employing the attentional cascade strategy, the novel face/eye detector was able to realize an analogous speed to Adaboost face/eye detector in this "close-range" application. The novel technique decided the class-specific threshold without causing any damage to the training data, and the validation data was able to encourage better performance. The novel technique is systematically assessed on O2FN, AR, and CAS-PEAL databases and contrasted with various techniques. When compared with the highly competitive system, built upon Adaboost face/eye detector and ERE approach for face recognition, the novel technique was able to decrease the overall equal error rate from 8.49% to 3.88% on the O2FN database, from 7.64% to 1.90% on the AR database and from 9.30% to 5.60% on the CAS-PEAL database. The innovative system was performed on O2 XDA Flame and on average it takes 1.03 s for the whole process, including face detection, eye detection and face verification.

Heather Crawford et al (2013), addressed two distinctive issues with de facto mobile device authentication, as furnished by a password or sketch. First, the device activity was allowed on an all-or-nothing basis, depending on whether the user effectively validated at the start of a session, without taking in to consideration the fact that tasks carried out on a mobile device had a variety of sensitivities, according to the character of the data and services accessed. Second, the users were tempted to re-authenticate recurrently in view of the bursty nature which represented the mobile device use. Owners responded by disabling the mechanism, or by selecting a feeble
"secret". To tackle the two challenges, they launched an extensible Transparent Authentication Framework which incorporated multiple behavioural biometrics with traditional authentication to perform an easy and uninterrupted authentication mechanism. The safety and usability estimation of the novel framework illustrated that a legitimate device owner was able to carry out all device tasks, when required to validate overtly 67% less frequently than in the absence of a transparent authentication technique. Also, the assessment proved that ambushers were immediately prohibited from accessing the on-device tasks as their behavioral biometrics was gathered. The enthusing outcomes backed the formation of a working prototype of the novel framework and gave support for added research into apparent validation on mobile devices.

ElieKhoury et al (2014) put in their best efforts to investigate the problem of a face, speaker and bi-modal authentication in mobile scenarios accompanied by incredible condition disparity. They introduced the disparity by enrolling client models on superior quality biometric samples gathered on a laptop computer and validating them on inferior quality biometric samples achieved with a mobile phone. For conducting these tests, they designed three authentication protocols for the mammoth publicly available MOBIO database. They estimated the high-tech face, speaker, and bi-modal authentication methods and illustrated that inter-session variability modeling using the Gaussian mixture models offered a constantly vigorous system for the face, speaker, and bi-modal validation. It was also illustrated that the multi-algorithm combination offered a reliable performance augmentation for face, speaker and bi-modal validation. Using this bi-modal multi-algorithm mechanism they achieved a hi-tech validation mechanism which achieved a half total error rate of 6.3% and 1.9% for Female and Male trials, correspondingly.
Wen Chung Kuo et al (2014) proposed an effective and reliable anonymous authentication technique for the mobility networks. To block the exposure of confidential data, investigators launched several unknown roaming authentication methods which employed diverse techniques to offer the integral security properties, such as the symmetric and asymmetric encryption, digital signature, and timestamp and so on. However, certain techniques continue to face safety and efficiency dilemma. So as to offer tripartite authentication and improve efficiency they established an innovative method to improve the efficiency and security vis-a-vis prior techniques.

Haowei Liu et al (2015), proposed algorithms for mobile platforms with Face Detection and Recognition on Mobile Devices. The innovative hands-on guide facilitated the engineers to comprehend the implications and issues of every design choice. They furnished a general idea of a domain of computer vision and boosted the design of computer vision applications on mobile platforms. Taking face-related algorithms as an instance, they conducted surveys and demonstrated how design choices and algorithms could be used for designing power-saving and effective applications on resource-constrained mobile platforms.

2.3 GAP ANALYSIS

M-commerce can effectively discharge its duty of delivering the products and services through wireless technologies to make the possible internet. However, the existing system in M-commerce has certain security vulnerabilities and not accurate for electronic transactions via mobile phone devices. Table 2.1 provides a taxonomy of various problems encountered in four M-commerce applications derived from the literature review.
Table 2.1 Taxonomy of problems encountered in M-commerce applications

<table>
<thead>
<tr>
<th>M-commerce applications</th>
<th>Mobile commerce systems</th>
<th>Mobile handheld devices</th>
<th>Protocol</th>
<th>Mobile payment Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal enforceability of contracts</td>
<td>Weak and Unreliable connectivity</td>
<td>WAP gap</td>
<td>Hacker can easily acquire PIN number from mobile phones</td>
<td></td>
</tr>
<tr>
<td>User protection</td>
<td>Limited processing Power and memory</td>
<td>It can enhance the resilience to Network perturbations</td>
<td>OTP generation can delay the payment process</td>
<td></td>
</tr>
<tr>
<td>Privacy of data (no unnecessary, unauthorized data collection)</td>
<td>Limited battery Operation time</td>
<td>Realizing superior Commit rates,</td>
<td>Undistributed PIN Processed by single server</td>
<td></td>
</tr>
<tr>
<td>Confidentiality of data (protecting authorized Data from misuse)</td>
<td>Very limited inputs.</td>
<td>It can increase the Wireless message cost and the blocking of transaction participants resulting in the lower transactions throughput.</td>
<td>Existing cryptographic Algorithms used in M-commerce system delays the payment process</td>
<td></td>
</tr>
<tr>
<td>Right of self-determination (to carry out or reject A communication).</td>
<td></td>
<td></td>
<td>Security issues with Existing cryptographic algorithms</td>
<td></td>
</tr>
</tbody>
</table>
So in an emerging world, mobile user and service provider authentication security levels have to be increased to fulfill the requirement of the secure M-commerce transactions. Few M-Commerce system focuses on login type of user authentication, if it’s a new user and directly logs in if he is an registered user (example: Flipkart, Snapdeal) and existing system doesn’t invoke fingerprint-based biometric authentication in an efficient way for mobile purchasing/payment services (example: iPhone6, Galaxy S6 have biometric scanner for accessing the phone but we propose to access the same biometric scanner while accessing M-commerce applications). Many Mobile commerce applications mostly utilized the registration and OTP techniques in M-commerce system for user authentication which is more vulnerable to payment modes.

To deal with the above problems mentioned, several approaches have been used which include:

- Decreasing, the load of complex computations to a server
- Reducing network traffic with better protocols
- Allowing cryptography algorithms to run in offline mode
- Developing cryptography algorithms w.r.t throughput
- Adding specialized chips to perform cryptography

However, the existing system that has been used for Mobile purchasing/payment services in handheld devices is not implemented and analyzed in an efficient way. That is the existing system is not secure and accurate for M-payments applications. To do such a transaction successfully, a secure environment is needed, and this important factor has to be considered.
in M-commerce transactions. So implementing high security in M-commerce applications would invite many users to perform M-payment/transactions immediately and irrespective of infrastructures. Hence in this work, secure, efficient and accurate M-commerce architecture is proposed for M-commerce applications.

2.4 PROPOSED ARCHITECTURE

![Proposed M-Commerce Architecture Diagram](image)

**Figure 2.1 Overall M-Commerce Proposed Architecture Diagram**

The proposed architecture is focused on secure transactions in M-commerce among users, financial institutions (bank) and service providers
(merchant). The overall system design is shown in Figure 2.1: The Proposed Architecture workflow is stated below in the following steps:

1. Customer (user) sends his details along with required product details to the service provider through the WAP gateway.

2. The service provider verifies the details of the product & customer and sends to the biometric server through the WAP gateway.

3. Biometric Server requests the customer details (fingerprint) from the customer.

4. Customer sends his/her fingerprint image to the biometric server through WAP gateway in a secure way using DWT technique.

5. The biometric server sends the comparison result details (matching score) to the service provider. Analyzing the matching score, service provider decides whether to access or deny the process of the respective customer.

6. Once the user is authenticated to proceed, the PIN distribution process is initiated.

7. The user PIN is transformed into an alphanumeric form using a unique sequence table. The user PIN, user ID, time stamp and IP address are tracked during the transaction. Also, the PIN is distributed in a secure way using the double encryption technique for PIN authentication.

8. The result is sent to the bank for transaction process as an OK or Not OK message.
9. The merchant receives the payment from the financial institution.

10. Finally, merchant delivers the order to customer

2.5 SUMMARY OF RESEARCH GAPS AND PROPOSED SOLUTIONS

This chapter reviews the issues related to problems encountered in the security of M-commerce. There exist several pieces of literature on Biometric Authentication, PIN Authentication and bandwidth limitation issues in M-commerce transactions. So using mobile-based applications securely in M-commerce transactions, it is important to circumvent this security constraint in both mobile networks and devices. This proposed architecture solves many problems encountered in current M-Commerce security systems.

One of the problems encountered is that they are not focusing on user authentication and also the existing system does not analyze fingerprint matching and feature extraction techniques in an efficient way for mobile purchasing/payment services. In addition, it is not secure and accurate for mobile payments applications. To welcome many users to perform mobile transactions, it is important to enable high security by providing secure identity authentication. Hence, this research work is focused on the implementation of secure M-commerce architecture by including an effective user authentication, PIN (personal identification number) distribution and cryptography technique for mobile payment/transactions.

In case of existing systems, for fingerprint extraction, only one feature extraction method is being used; but in our research we have used two feature extraction techniques for fingerprint extraction which improves accuracy.
In case of existing systems, PIN is not distributed and only authentication server is being used for processing PIN; however, in our proposed research, PIN is distributed in two halves and processed by two server namely-authentication and external server which enhances integrity.

Double encryption method has been used for PIN transaction in our proposed research which improves confidentiality. This method has not been used in existing systems. The designing of such a kind of secure architecture in M-commerce is essential and that will invite more users to perform mobile payments/transactions with confidence. This can be achieved by designing an effective M-commerce architecture with secure user authentication and service provider authentication.

Next chapter overviews about the biometric authentication system, various types of biometrics and its implications in our proposed work. Fingerprint is considered to be the best and fastest method for biometric identification. Hence, the fingerprint recognition based biometric methodology is adopted on the part of user authentication side for improving security levels.