ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.4

Secured Cardless Payment Method using Bluetooth Technology

Jayashree .S[1], Keerthana .K[2], Kesharvi .S[3], Mythili .D[4], Mahalaksmi .M[5]
UG Student[1, 2, 3, 4], Associate Professor[5]
Department of ECE
Velammal Engineering College,Chennai,Tamil Nadu, India

Abstract:
In daily life people use credit cards for shopping, check card, bus card, subway card for traveling, student card for library and department, and many kinds of cards for unlimited purposes and etc. So problem is that a person has to take many cards and has to remember their passwords or secret codes and to keep secure to take with him all time. Wireless technologies provide a new channel of implementation. In this regard, the potential of short-range wireless technologies such as Bluetooth is enormous. These systems can be used for proximity payment to vending machines or offering banking service in the bank area. However, unsolved security issues are the biggest barriers to the growth of mobile payment. This paper is focused on the security of banking services which can be offered through Bluetooth technology.

1.INTRODUCTION

In today's world everybody have number of cards in their pocket or purse for purchasing and selling things, traveling and many facilities for his need. The problem is that the person have to pick many cards and he also has many secret codes and with other tensions too, so to avoid these kinds of problems the biometric fingerprints payment technique is used for easy utilization. Fingerprint authentication is still the number one choice of security measure for identity verification in Malaysia and Singapore, according to a Unisys survey. [1] SINGAPORE--Citibank on Wednesday 9th November 2006 launched a new fingerprint authentication payment service that lets its credit card customers pay for goods and services with a touch of the finger. [2] In the future, no one will need pockets to keep keys, credit cards, checkbooks, rather than it will be replaced by something closer to the body. When you need to open something, make purchases, mostly you'll do it with a fingerprint, a voice command, or a computer scan of your eyeball.. Pay By Touch, specializes in biometrics. Elementary schools are installing iris scanners to keep out intruders. Companies increasingly use fingerprint scanners to authenticate computer users. "You won't need cash or cards to pay for anything. All you need is your finger". Among many applications, transit services represent a major application area for mobile payment systems, as demonstrated by the above discussion. In addition, many organizations, such as transit agencies, financial institutions, mobile carriers, and providers of smart cards, are involved in mobile payment systems for mass transit. In existing transit service systems, passengers' private information, such as their identity and route, can be revealed to such organizations, and they may share this information to balance accounts. However, it is difficult to ensure that the mishandling of passengers' private information by these organizations does not occur. This information can provide firms with various benefits; however, passengers may want to keep such information private. In other words, passengers' identities and routes should remain anonymous while organizations balance their accounts, which is called *anonymous balancing*. *Fair mobile payment protocols ensure that both participants can engage in the exchange without the risk of suffering a disadvantage (e.g., losing their money without receiving anything for it).* Mobile payment is payment via a mobile device which includes mobile phone, PDA, and mobile computer etc. Mobile payment ensures that neither party involved in the payment is in danger of suffering a disadvantage, like losing its money. If a vendor sends for example a music file to a customer, there is no guarantee that it will reach the latter within a certain time. Consequently, mobile payment protocols can merely guarantee eventual delivery of an item assuming that the network communication will eventually be reestablished. Eventual delivery though is too weak for items that lose value over time, like location dependent information. Such items which lose their value over time are called time sensitive [3].

2.LITERATURE SURVEY:

2.1 An Investigation on Multiple e-Payments and Micro-Payment – A Technical and Market View William Song, Framkom, Electrum, S-164 28 Kista, Sweden:

E-Payment is the corner stone of an e-commerce system. With respect to different payment requirements, different e-payment techniques and methods are developed with specific application purposes. E-payment technology involves digitized cash, e-wallet, electronic credit/debit card payments. However, in the B2C e-commerce, e-payment has not reached a massive market yet. There are many reasons behind this. One of the reasons is lack of multiple channels for payment. Another difficulty is enlarging of micropayment market. Both strongly hinder a wider acceptance of e-payment. we present an investigation on multiple e-payment and micro-payment from the technical point of view of and market

2.2 A simple two-sided market model with side-payments and ISP service classes George Kesidis CS&E and EE Depts, The Pennsylvania State University, University Park:

We consider a simple two-sided market model of an Internet Service (access) Provider (ISP) and Content Provider (CP, over commodity Internet access) on a platform of user demand. Though the model does not consider provider competition and resource congestion, it does consider advertising revenue, multiple ISP service classes, separate price sensitives for each provider type, and side-payments from CP to ISP. We argue that side-payments are effectively in play even under network-

neutrality regulations owing to considerations in Service-Level Agreements (SLAs) of asymmetries in traffic aggregates at boundaries (NNIs) between eyeball ISPs and transit ISPs, the latter serving the CPs remote to the eyeball ISPs. Finally, we consider a game between content providers based on "managed" and commodity-Internet-access services.

2.3 Expanding Renewables and the Challenge of Designing Market Payments:

Under higher levels of variability, conventional generating units are required to operate over a broader range of outputs and to startup and shutdown more frequently. Thus, when new units with limited operational flexibility are introduced, they will tend to impose costs on the rest of the generating units. Therefore the value of a generation resource to a system is not only a function of its own costs, but also increasingly the extent to which it imposes costs on other units. Future market incentive structures should therefore not specifically target the generating units with the lowest costs, but rather those units that result in the lowest overall costs for the whole system. As an example, this paper investigates the degree to which profit-maximizing investments under an energy-only, opportunity-cost bidding market structure, depart from the cost-minimizing, socially-optimal investment trajectory, under increasing levels of wind power.

2.4 Game between mobile operators and financial institutions in mobile payment market:

The game between bounded rational mobile operators and financial institutions is studied on the basis of evolutionary game theory. Then, the factors influencing the cooperation between mobile operators and financial institutions are analyzed. The result shows that cooperation between mobile operators and financial institutions is the trend; moreover, the probability of cooperation of both sides has a positive relation with excess income of cooperation and independent product development and a negative relation with the research cost and betrayal income; reasonable proportion of excess income allocation will effectively benefit both sides and achieve a win-win situation.

2.5 Electricity Markets with Payments for Engaged Capacity

One peculiarity of the wholesale electricity market that seems persistent across some market designs is the"missing money" problem. This problem appears when generators do not recover their costs given the market price of electricity. The "missing money" problem may be in part due to the pricing and payment mechanisms set in place. Competitive forces should set the price of a commodity to the marginal cost of the marginal unit producing the good if the functions are convex. However, electricity markets are characterized for having non-convex function due to the generators' minimum and maximum outputs constraints, start up and shut down costs, amongst other characteristics. Therefore, uniform marginal price schemes will not always create market-clearing price. Under this scheme, not all the generators will cover the costs incurred in production. Different recovery mechanisms have been proposes, but the case of the "missing money" is still a challenge these days, especially in pool-based markets. A possible solution is to price for capacity as well as for the electricity. Capacity markets have developed, and they still are in progress. And although some authors are not supporters of capacity payments and capacity markets, some others have shown the need for capacity payments and suggested a design for its market. This paper contributes to the growing literature in capacity pricing by suggesting a new approach to obtain electricity prices and capacity prices for the plants engaged into production. This approach applies the semi-LaGrange an methodology to an expanded Unit Commitment and Dispatch Problem. The new semi-LaGrange an problem is solved by using a sub gradient approach. We obtain a set of prices for electricity and capacity that are high enough to cover the generators' costs, as well as sending the right signals to the market, and producing efficiently at a minimum costs. We believe that the excess revenue obtained with this approach can be used as a guide to future investment, and as a consequence, can help to find the "missing money"

3. SECURING BLUETOOTH-BASED PAYMENT SYSTEM

Mobile payments represent an opportunity for the mobile industry and for financial service companies. It has been welcomed in most of the countries as a new branch in electronic banking while it has some superiority over e-banking due to its availability, High penetration coefficient and being fully personalized. Financial establishments have also begun implementing mobile banking applications utilizing Bluetooth. According to recent research by the Celent financial advisory firm, 200,000 US households use some form of mobile banking. By 2010, the market is expected to grow to 17 million US households. In Mexico, BBVA Bancomer has deployed more than 13,000 Bluetooth enabled payment terminals [3]. EUROCARD is another form of Bluetooth based wireless payment has been used in Sweden [4]. Mobile payment provides flexibility and convenience for consumers. However, mobile banking via Bluetooth presents a risk. While no generic profile for mobile banking exists for Bluetooth, application developers must design systems with security in mind and require a protection mechanism for detecting malicious Bluetooth traffic. In this part,we elaborate some application of Bluetooth technology in mobile payment.

3.1 Proximity payments using Bluetooth

Mobile proximity payments are predicted as the best medium term revenue opportunity. One of the main applications of Bluetooth technology can be defined in proximity payments which involve the use of wireless technologies to pay for goods and services over short distances. Proximity transactions develop the potential of mobile commerce, for example, using a mobile device to pay at a point of sale, vending machine, ticket machine, market, parking, and so forth. Through short range messaging protocols such as Bluetooth, the mobile device is transformed to a sophisticated terminal that can process both micro and macro payments. In proximity [5]

3.2. Banking services using Bluetooth.

Mobile banking is considered one of the most popular mcommerce applications. Banking services are generally divided into the four categories which all of them can be offered through Bluetooth technology. These services includes Notifications and alerts services which are offered to inform the customer of the transactions done or to be done with his account, Information services concerning transactions and the amount of money available in customer's account are sent at certain intervals, Applications services in which an application is sent to the server concerning the account or special transaction and services through which banks can transfer amount of money between customer's accounts or pay an amount to a third party such as paying bills . The main goal of using Bluetooth in m-banking is to offer banking services in bank area through mobile phone without paying for any costs

in order to decrease the rush hours and amount of banking operations done by the bank clerks .In this method bank customers can be connected to server 22 installed inside the bank through Bluetooth technology and to handle their banking affairs through their mobile phones. This server will be capable to offer banking services through Bluetooth technology by which the server can be connected with other devices equipped with Bluetooth lying in 100-meter scope [6]. Offering banking services through Bluetooth can have many advantages:

- Mobile phones are widely used by people all the time and Most of them are equipped with Bluetooth technology (Availability).
- Security of this service is higher than internet, and SMS because of its limited Scope [6].
- Due to low-speed and high-cost of internet for mobile phones in some countries like Iran, using this service is almost fast and does not incur any cost.
- Bluetooth technology makes it possible to offer mbanking services to several people in accordance with the number of servers [7].
- Payment systems using Bluetooth not only decreases visits to interior of the banks but also can decrease some visits to ATMs for handling such affairs as inspection and checking of account balance and alleviate problems of these appliances.[6]

3.3. Security issues in Bluetooth applications

Security and privacy are essential elements for the success of mobile commerce and its applications specifically in payment area. As with any wireless technology, Bluetooth has several inherent security risks because access to any Bluetooth device is potentially open to anyone in the range of the device. Thus Bluetooth security is a huge concern for wireless applications [8]. In this part, we introduce some of the known vulnerabilities toward Bluetooth application and then we propose our solution based on honeypot systems to detect and delay some of these attacks.

3.3.1 Bluetooth-Enabled Attacks

Bluetooth-Enabled Attacks can be classified from different points of view. One of the major weaknesses of any wireless technology like Bluetooth is that its physical medium is based on radio frequency (RF). Because Bluetooth transmissions must travel through the air in the form of RF waves, they are prone to Denial of Service (DoS) attacks. An attacker simply to generate enough RF noise in the Bluetooth network frequency to saturate the medium and made impossible the establishment of any communication [9]. In disclosure threats for example, Bluetooth air sniffers make it possible to sniff the raw data being exchanged between two devices. Such attacks could have a serious impact on the security of m-payment schemes. But the most important attacks in Bluetooth networks is *wardriving* which refers to any type of attack that attempts to gather information about a Bluetooth-enabled device in order to proceed with further attacks. Successful wardriving detection allows targets to take countermeasures prior to follow-on attacks [10].There is several different ways to prevent Bluetooth-based devices from being the target of any of the attacks launch via Bluetooth. Fortunately not every Bluetooth device is susceptible for every attack and most of these treats cannot be launched unless the devices are discoverable to attackers. So the best defense against these threats is to limit device discoverability and connectability [11]. In the next section, we present a honeypot system which can be used as a deception to make the discovery process much longer.

3.4 Using Honeypot concept

Information security is a growing concern today for organizations and individuals alike. This has led to growing interest in more aggressive forms of defense to supplement the existing methods. One of these methods involves the use of honeypots which are mainly used to attract attackers to study their behavior and to learn their tactics. For computing, a honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource [12]. By being a vulnerable and well-situated entity, the honeypot appears to have value and be an easy target for attackers. In other word, by standing up honeypot targets, we can distract attackers from more valuable machines on the network. Honeypots are closely monitored and any actions directed towards them are by default suspect [13]. These systems can be classified based on different aspect such as their purpose, and level of interaction with the attackers (Table 1).

Table 1. Honeypot classification Properties

Environment:	Production	Research	
Interaction:	Low	Medium	High
Purpose:	Deception	Deterrence	Detection
Attacker:	Script	Professional	
Profile:	Kiddie	Blackhat	

Honeypots are a relatively new technology that is becoming increasingly popular as commercial solution. While recent work [21, 22] identifies Bluetooth payments as a potentially forthcoming area of security issues, we find honeypots to be tools that can help us in *prevention, early detection and Deterrence* of malicious attacks by studying malicious and unauthorized behavior. However, we need to ensure that the honeypots follow desirable characteristics to interact with attackers in Bluetooth network.

4. ANONYMOUS DIGITAL CASH PROTOCOL

Accountable anonymity means the valid digital cash cannot reveal the customer's identity, but which can be detected if the cash is double spent. In this section we propose a new offline digital cash protocol adapting to mobile payment. And it utilizes smart card to guarantee anonymity of digital cash.

The smart card based digital cash protocol

In a digital cash system we have three kinds of actors: a financial network such as a bank, a payer or customer, and a payee or a vendor. There are three different types of transactions during a digital cash procedure:

a) Withdrawal, in which the customer transfers some of her digital cash from her bank account to her wallet (it could be a smart card in the mobile device).

b) Payment, in which the customer transfers digital cash from her wallet to the vendor.

c) Deposit, in which the vendor transfers the digital cash he has received to his bank account. As Fig.1 shows, if the customer wants to get anonymous cashes she requests the anonymity provider agent to blind the cash. So binding digital cash sub protocol is introduced.

Employing smart card as a distributed anonymous provider agent

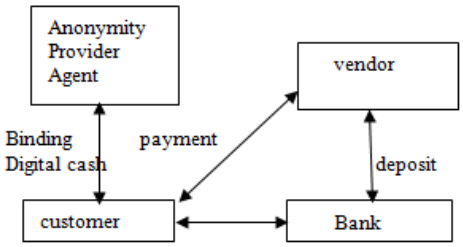

Figure.1. An anonymous digital cash protocol

The smart card can be embedded into a customer's mobile device. To communicate with a regular computer such as a vendor the card is assumed to have a distinguished interface, meaning that only predefined operations can be invoked with carefully chosen input and output parameters. The communication between protect the integrity and confidentiality of messages. The smart card is issued by a bank. If a smart card shall serve as a distributed anonymity provider, we have to presume that it fulfills the following requirements:

− Tamper-resistance. The smart card must be protected so that it is impossible to read out secret data or to change the behavior of the card.

− Authenticity of messages.

Anybody connecting to this card must be able to check the authenticity of all messages generated by it. This can be achieved, if the smart card contains a private key to generate digital signatures. The corresponding public key for the card's signature must be certified by some trusted authority, probably a bank. Furthermore, a smart card should be able to identify the sender of messages by using digital signatures. Therefore, the card must possess some built-in authentication information, e.g., the public key of a trusted certification authority. The card can then validate the customer's or the vendor's public key certificate. This prevents the smart card from being fooled by an attack who claims to be somebody else. There are some benefits of utilizing a smart card:

− Some of drawbacks of an anonymity provider server can be alleviated by placing its functionality "closer" to the participating parties, making the quality of communication more predictable. It increases the availability of anonymity provider agent to an extent where timely blinding digital cash and changing for cash are feasible.

− The smart card only serves for a unique customer. So a trusted hardware device local to the customer is much less endangered to become a bottleneck since a customer does usually not engage in more than one transaction concurrently.

− The assumptions about the security of the smart card (e.g. it is tamper-proof) ensure correct protocol execution and its verifiability for both parties.

− The smart card is scalable. We can utilize smart card on the customer's side partly taking over the duties of the TTP (trusted third party) to support fair exchange in mobile environments.

4.1 PAYMENT AND TRANSACTION PROCES

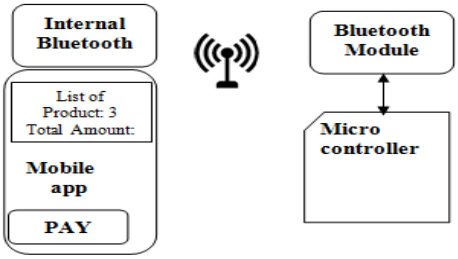

Figure.2. Payment process

The following steps are carried out as per figure, The ATM card is scanned and the details are stored in the mobile phone application. Then the details are checked and saved. During the payment process, the sender's mobile phone is connected to the receiver side devices like an ATM machine or card swiping machine using Bluetooth. Then the required details are entered using the Arduino micro controller.

5. BIOMETRIC SECURITY

Biometric values can identify people by measuring some aspect of individual anatomy, behavioral characteristics or ingrained skills. Biometric authentication technology such as face, finger, hand, iris and voice recognition are commercially all participants and the smart card is expected to be secure, i.e., cryptographic mechanisms are in place to available and many organizations such as banks, healthcare and government are using biometric to verify an individual's identity. Biometric system usually works on pattern recognition which is acquired from an individual, and comparing this feature set against the template which may be either stored in database or inside the chip. A comparative result of several biometric traits with different biometric technologies has been compared and present in table 1 based on these traits best suitable biometric technology for payment cards is identified. Fingerprint technology when compared to others has an extra edge as there is no trait which is low in one of the categories [14]. Biometric security have the potential to add valuable layer of security to payment card industry. We cannot store clear text biometric image or biometric template alone in the chip card, as they are prone to attack. Some of the well-known biometric attacks are skimming the biometric identity. Biometrics is good at identity verification with better protection against repudiation, but if deployed alone it may not provide high level of security. On the other hand cryptography provides security, privacy and anonymity and when combined they provide the basis for a better verification mechanism for EMV cardholders. Researchers have combined cryptography and fingerprint security and named it as fingerprint vault [15]. Where incorporating random phase mask and logistic map can further increase the security [16]. The biometric security using fingerprinting and encryption by cryptography is the solution for all the security threats presently being faced in CHIP and PIN cards. The trailing section presents all the feasible methods for implementing finger printing based biometric security in cards.

5.1 METHODS OF IMPLEMENTING FINGERPRINT SECUIRTY:

Moving from one security mechanism to another has never been easy, it requires time, cost and other factors. The most important thing need to be considered is the risk associated with it, especially when it comes to payment cards. The integration of CHIP and PIN technology was not an easy task, it required lot of analysis be it cost, time and risk. When integrating fingerprint security in payment cards there are two factors which need to be considered: CHIP space complexity and time complexity. Fingerprint can be stored either in payment card or in a central database. To store the data in the payment card (similar to current DDA and CDA cards for PIN storage) sufficient storage capacity is needed. Local storage on the chip will offer more privacy and portability for the user and will ensure the template remains secret with the cardholder (in the secure area of the chip). This design would require payment cards to have sufficient memory to store the encrypted fingerprint template. The current available payment

cards have 8K of available non-volatile memory half of which is occupied with authenticator certificates. The EMV and related chip card specifications define the physical, electrical, data and application level of payment transactions. The storing of fingerprint data can be either store as raw fingerprint (in form of bitmap image) which is not secure or a template of fingerprint can be securely stored. A complete fingerprint image (bitmap format) is around 50K to100K, which cannot be stored in current payment cards, while a fingerprint template requires only 300byte to 2K memory space which will fit on current cards. Most of the smartcard applications that are using biometric security are using biometric templates. So the current CHIP in payment cards have sufficient memory to store encrypted fingerprint template together with issuer and cardholder certificates. The interoperability and performance characteristics for proprietary and interoperable templates are reported in [17]. As far as approaches for implementing crypto-biometric in smart cards is concern there are two such approaches. These approaches are similar to what has been implemented to chip and pin technology in DDA/CDA environment. The first one is matching fingerprint online named in this paper as type –I and the second approach is matching fingerprint in hybrid environment that is offline/online named as type-II.

A.Online Card Authentication (Type-I)

In this approach template of the fingerprint is stored in database of the card issuer. The user needs to present a matching template in order to authorize transaction. Visa in collaboration with UIDAI is implementing this method. In this method user's VISA account is linked to Aadhaar card also called as unique identity card which act as a reference for the biometric data associated with that account. During the authentication phase user record is first selected using the aadhaar number and then biometric inputs are matched against stored data (template) which was taken from the user at the time of enrollment of Adhaar card [18]. Major drawback of this method is that it doesn't allow offline transactions where in current DDA/CDA EMV environment transactions have cardholder authentication processed offline. This method when integrated in payment cards is called Match-off-Card technology, in which the original template can be stored in the database, so during enrollment a fingerprint reference is stored in the CHIP of payment card [19]. During authentication, biometric reader attached to POS or ATM will generate a biometric template, encrypt it with public key of the CHIP (DDA/CDA cards) and send it to CHIP of payment card for processing. The CHIP then decrypts the template and again encrypt template with a reference number and digital signatures of issuing authority and send it to issuer for verification. Once the encrypted message is received by issuer it is decrypted to obtain the fingerprint template which is then compared to the fingerprint template stored against the received reference number.

B. Offline/Online Card Authentication (Type-II)

This approach can be used to authenticate the cardholder in both offline and online environment. In the future, there are two ways to implemented this.

I) Fingerprint reader embedded inside card (Type-IIa):

Paul J. Baratelli first invented smart card with integrated fingerprint reader [20]. In this approach payment card has inbuilt optical reader which stores fingerprint template. This method is similar to fingerprint reader compatible smart phones. The template is just a representation of part of the fingerprint and it is not a stored image. This is one of the major advantages of using this approach in implementing. When fingerprint is scanned the advance system runs this template through a cryptographic hashing algorithm and stores the result. During hashing the template is combined with unique or random number to enhance its security.

II) Fingerprint reader integrated with POS and ATM's:

In this approach the fingerprint image or fingerprint template hash is encrypted and stored inside chip of the card during user registration process. User need to insert the card in POS with fingerprint scanner attached and then users have to tap their finger to generate a fingerprint template which is then encrypted and send to chip of the card for authentication (the same as when sending a PIN to the CHIP in DDA and CDA). This method can be integrated in payment card with two different style either using match-on-card technology] or template-on-card technology. Match-on-card technology is the one in which the fingerprint is scanned at the time of enrollment for the card at the financial institution. A template is generated using an algorithm and is encrypted and stored in payment card. During the authentication process fingerprint is scanned at the reader side and a template is generated which is then encrypted and send to the card for matching. Match results are calculated inside the payment card. Match-on-card technology should be considered for implementation when the card is expected to be used in a setting where the POS is vulnerable to tampering making it an untrusted device. In most cases POS terminals in merchant stores should not be viewed as trusted devices as they are not monitored on a continuous basis.

5.2 BENEFITS OF FINGERPRINTING SECURITY

A.Enhanced Privacy

The fingerprint cannot be borrowed, lost or stolen like a PIN and so strengthen the authentication of an individual's identity. Fingerprint security would ensure that only the rightful cardholder can have authorized access to the personal information stored inside the card. Fingerprint security will also increase trustworthiness of POS and ATM terminals, as the authentication process remain secure, also while using DDA/CDA cards the communication between the terminal and payment card is always encrypted.

B.Enhanced Security

Fingerprint template can be digitally signed and stored on the payment card at the time of enrollment and is processed inside the payment card when used. Cardholder authentication can be performed by the payment card comparing the live template with the template stored in the card. The fingerprint template never leaves the card, protecting the information being accessed therefore enchasing the security of the payment card. Payment cards have sufficient memory to store one or more fingerprint template and multiple cryptographic keys to provide more security to the cards. Fingerprint cannot be shoulder surfed so it can provide more security and can be safely used at POS and ATM's.

C..Upgradability

Ability for a system to be upgraded without needing large investment in a new infrastructure is a key requirement in any identification system. Costs of implementation and transaction time are some of the important factors which need to consider when deploying new infrastructure for payment cards. Cost should not be a bigger issue as the current payment cards are

having sufficient memory to store fingerprint template thus can save cost by avoiding large memory. The cost associate with card depends on its type. A type-IIa card would require a fingerprint reader inside the card but would not require upgrading the POS and ATM's. Table 2 present fingerprinting security technology capability to tackle threats and vulnerability faced in the PIN security technology.

Table.2. Comparativing pin security with fingerprint security

FEATURES	TECHNOLOGY	
	Chip and PIN	**FINGERPRINT**
security	Eavesdropping and shoulder sniffing attacks are possible, more secure in DDA/CDA environment then SDA	More secure than PIN as fingerprint template is used
security	PIN can be extracted using skimming tool	Recsontrition of original fingerprint is not possible
security	New PIN can be assigned if Compromised	New fingerprint template are created if compromised
time	Transaction time would be more compared to fingerprint security as user need to enter PIN for verification	Transaction time will be less as compared to PIN as user would only need to scan fingerprint
cost memory	Less expensive technology 8Kb of memory required in the CHIP.	More expensive, fingerprint scanner is required Same memory and no need to replace the existing card
Technology acceptance	Accepted in most of the countries as replacement to less secure magnetic stripe	Technology used by many government and private organization worldwide
limitation	PIN can be forgotten and once lost it can only be reset from issuer and require other authentication	fingerprint cannot be lost, only possible if case of disability associated with fingerprint

6. CONCLUSION:

Basically, most of the problem with card payment starts from the fact that the payer's identity - needs to be established in the card-not-present mode. This is inherently problematic because it's at odds with the original use of cards (where the card and cardholder are present at the moment of purchase). It also implies that, for instance, chip-and-PIN isn't available to establish the payer's identity. This is exacerbated by the fact that the Internet facilitates distribution of guesses for data fields over many merchant sites. To prevent this attack, either standardization or centralization can be pursued (some card payment networks already provide this). Standardization would imply that all merchants need to offer the same payment interface, that is, the same number of fields. Then the attack doesn't scale. Centralization is achieved by using payment gateways or card payment networks. Neither standardization nor centralization naturally fits the flexibility and freedom of choice one associates with the Internet or successful commercial activity, but the two will provide the required protection. It's up to the various stakeholders to determine the case for and timing of such solution

7. REFERENCES:

[1]. G. Ateniese, D. Song, and G. Tsudik, "Quasi-efficient revocation of group signatures," IACR Cryptol. ePrint Arch., Tech. Rep. 2001:101, 2001. [Online]. Available: http://eprint.iacr.org/2001/101.

[2]. D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Advances in Cryptology—CRYPTO (Lecture Notes in Computer Science), vol. 3152, M. K. Franklin, Ed. Berlin, Germany: Springer, 2004, pp. 41–55.

[3]. Mexican bank deploys hypercom bluetooth-enabled payment stations. Mobile Enterprise Magazine.Oct 2007.

[4]. Gustafsson L. (2004), Eurocard Bluetooth Payments interview, J. Chen, Ed.

[5]. Agarwal S., Khapra M., Menezes B. and Uchat N. (2007), Security Issues in Mobile Payment Systems.

[6]. Shahreza,M. and Shahreza M. H. (2007), Mobile Banking Services in the Bank Area, SICE Annual Conference, Japan

[7]. Chen J.J., Adams C. (2004), Short-range Wireless Technologies with Mobile Payments Systems, ACM.

[8]. K. Pousttchi, and M. Schurig (2004), Assessment of today's mobile banking applications from the view of customer requirements, Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 5-8.

[9]. Potter B. (2003), "Bluetooth - Security Optional," *Network Security*, no. 5, pp. 4-5.

[10]. Suen Yek (2003), Measuring the Effectiveness of Deception in a Wireless Honeypot, 1st Australian Computer, Network & Information Forensics Conference, Australia.

[11].Johnson K., Zuroff M., Whitaker J., Bluetooth Security, By MJK Group

[12].Spitzner, L. (2003). Honeypots - tracking hackers. Boston: Pearson Education Inc.

[13]. Barfar A. and Mohammadi S. (2007). Honeypots: Intrusion deception, ISSA Journal.

[14]. Smart Payment Association (SPA) - Biometrics for Payment - APosition Paper - November 2013 [Online] Available: http://www.smartpayme ntassociation.com/en/publications_001/white_papers/biometrics-for-financial services---a-spa-white-pa_hqrt81y8.html[Accessed: Dec. 15, 2015]

[15]. Thi Hanh Nguyen "A fingerprint fuzzy vault scheme using a fast chaff point generation algorithm" in Signal Processing, Communication and Computing (ICSPCC), 2013 IEEE International Conference., KunMing., 2013, pp. 1-6.

[16]. Delong Cui "A Novel Fingerprint Encryption Algorithm Based on Chaotic System and Fractional Fourier Transform" in Machine Vision and Human-Machine Interface (MVHI), 2010 International Conference., Kaifeng China, 2010, pp. 168-171.

[17]. MINEX II testing on biometric algorithms NIST IR 7477 [Online] Available: http://www.nist.gov /customcf/get_pdf.cfm?pub_id=908096 [Accessed: Feb. 18, 2015].

[18]. DERMALOG LF10 Fingerprint Scanner [Online] Available:http://www.dermalog .com/en/products_solutions/ fingerprint scanner/lf10.php [Accessed: Feb. 19, 2015].

[19]. International Standard ISO/IEC 24787 Information technology —Identification cards — On-card biometric comparison [Online]Available:http: //webstore.iec.ch/ preview /info _isoiec24787%7Bed1.0%7Den.pdf. [Accessed: Feb. 15, 2015].

[20]. Paul J. Baratelli, "Smart card with integrated fingerprint reader US. Patent 6325285 B1, Dec 4, 2001.

[21].Delong Cui "A Novel Fingerprint Encryption Algorithm Based on Chaotic System and Fractional Fourier Transform" in Machine Vision and Human-Machine Interface (MVHI), 2010 International Conference., Kaifeng China, 2010, pp. 168-171.

[22]. MasterCard Canada Press Section [Online] Available: http://www.mastercard.com/ca/company/en/security_risk.html [Accessed: Jan. 14, 2015]