International Journal of Innovative Computing, Information and Control
Volume **8**, Number **4**, April **2012**

ICIC International ©2012 ISSN 1349-4198
pp. 2747–2759

USABILITY BASED RELIABLE AND CASHLESS PAYMENT SYSTEM (RCPS)

Shafiq ur Rehman[1], Jane Coughlan[1] and Zahid Halim[2]

[1]School of Information Systems, Computing and Mathematics
Brunel University
Kingston Lane, Uxbridge, Middlesex UB8 3PH, United Kingdom
{ shafiq.rehman; jane-lisa.coughlan }@brunel.ac.uk

[2]Department of Computer Science
National University of Computer and Emerging Science
A.K. Brohi Road, Sec. H-11/4, Islamabad 44000, Pakistan
zahid.halim@nu.edu.pk

Received October 2010; revised February 2011

Abstract. *The advent of e-payment systems has promulgated considerable design and usability issues. These concerns have manifested themselves as the key inhibitors to the success of electronic payment systems. Credit and debit cards have proved to be popular alternatives to cash payments in retail transactions. However, this is merely due to the unavailability of a system that would provide a reasonable alternative to the threats posed in carrying them. We attempt to propose a system that provides a platform for cashless transactions based on reliability and usability features. The Reliable and Cashless Payment System (RCPS) entails the involvement of an accredited financial institution that invokes an element of trust essential to design of an effective payment system. In this paper we address the security flaws in modern payment systems and propose a model that would make possible payments without cash or credit cards. We do also consider HCI issues, usability concerns and soaring financial crime rate in our milieu.*

Keywords: RCPS, E-payment, Security, Usability, Macro payments, Micro payments, SET

1. Introduction.

With the brisk development of e-commerce, e-payment systems have evolved steadily in order to burgeon both online as well as offline trade transactions for payment settlement. The challenge for system developers is to model their applications in coherence with the fundamental principles of human computer interaction. Failure to incorporate proper usability, security and efficiency in system design results in complete rejection of the software product.

Abrazhevich and Rauterberg [1] reiterated the HCI stance on usability by advocating the provision of usability, privacy, security, and trust in building effective business oriented electronic payment systems. The advents of payment cards have seen a complete traversal from the conventional cash payment systems to a more secure online payment method. Payment cards thereby offered more utility and usability to the customer in facilitating consumer transactions and catering to both security and reliability needs.

The omnipresence of credit cards, however, posed immediate problems as hackers quickly went into operation tracking down credit card numbers from major retailers' data bank. The security feature that credit card vowed during the early age was soon no more present. Similarly, in countries where street crimes are on a high, card theft is an easy way to rob an individual from a huge amount of money which he would not normally carry in his wallet.

Electronic payment systems have failed to receive widespread acclaim due to non compliance of HCI principles. Abrazhevich and Rauterberg [2] have identified that there is still a very slow adoption rate of online electronic payment systems even in advanced countries. The research has reiterated the need for an electronic payment system that complies with the design principles of human computer interaction. This would include not only incorporation of usability features in system design but also involvement of high rated third parties and financial institutions, which could facilitate the process of establishing an e-payment system that would provide a total customer experience.

There has been considerable research done on the improvement of online payment facilities. However, a payment system that would cater to the needs of offline transaction settlement needs consideration. Credit and Debit Cards are normally employed to carry out Point of Sale (POS) transactions. However, a close study of usability and security reiterates the need of a convenient system that would have easy access for all, be cost effective (unlike credit cards that charge an annual fee and heavy interest) as well as provide necessary safeguard against external as well as internal security threats. Interestingly, the current electronic payment systems have to 'trade off' between one HCI variable or the other depending upon the type of use. In an environment where security threats are lurking due to poor economic as well as social conditions, it is imperative to formulate a payment system that provides ease of use, privacy, and above all security. The overwhelming use of credit cards has led to many cyber crimes by virtue of either a stolen credit card or misuse of credit card information of another user over the Internet.

Many online e-payment sites such as PayPal are exploring opportunities of providing the customers a complete experience. However, in a milieu where online transactions are limited and external security threats are omnipresent, it is imperative to design a system that would facilitate e-payment. This mechanism would not only provide convenience to the user but attempt to reduce loss in case of a street crime to a minimal level.

Particular ingredients in the success of e-payment systems would include security, reliability, responsiveness, and trust on service providers, easy access, and widespread acceptability. Our proposed system attempts to address all these issues. Figure 1 exhibits the current issues in the acceptability of e-payment systems world-wide.

1.1. Organization of paper.

The rest of the paper is organized as follows. Section 2 provides review of the related work. In Section 3, we explore the usability and security perspective in e-payment system. Section 4 outlines the methodology employed. In Section 5, we examine the HCI attributes of various e-payment systems and their limitations. In Section 6, we discuss the usability based reliable and cashless payment system (RCPS) in an offline environment. Section 7 identifies future direction of research, compares our model with some of the contemporary models and concludes the paper.

2. Related Work.

Considering the overwhelming popularity of electronic payment systems, there has been extensive research in recent years in order to propose possible models that would address security and usability concerns. Unless a model focuses on these two fundamental aspects, there would be little chance of luring customers into accepting the payment system as a viable business option. Most of the research has been on e-commerce applications in an online environment. In developing countries, where e-commerce is still a naïve technology, there is a need to introduce a tailor made system that can facilitate customer to business (C2B) transactions. Safeguards against external security threats need to be in place in order to propagate e-payment systems. Usability is also a feature that is extremely important as a complex system would be unwanted even if it has appropriate security procedures in place.

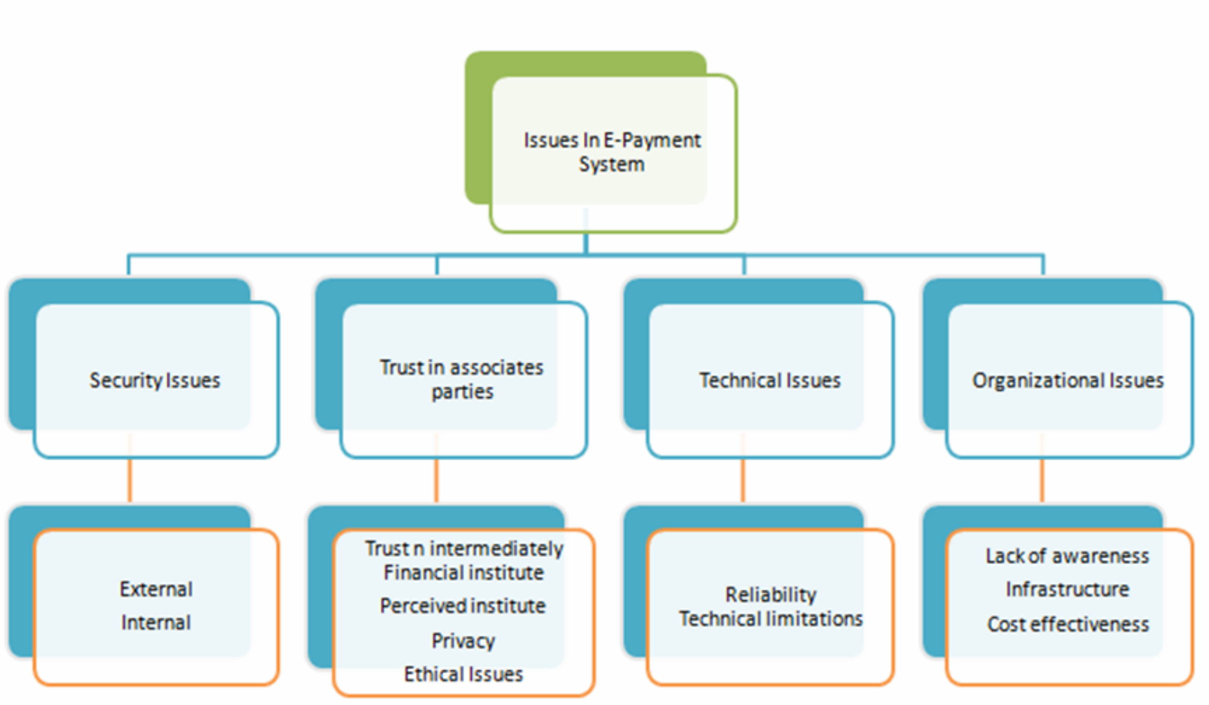

Figure 1. Current issues in the acceptability of e-payment systems world-wide

Bruno-Blitz [3] has identified lack of innovation and research in building e-payment systems online. According to the international standards assessment report, Internet banking and e payment sites have shown very little innovation and usability enhancement over the years. This is one of the reasons why the e-payment systems have failed to achieve world wide acceptance.

Silva [4] carried out a survey to delve into the consumer perception of e-payment. The results indicated an inclination towards on-site payments and purchasing rather than using e-commerce and Internet banking for day to day transactions. A consumer perception of inadequate security design that creates an element of risk in e-payment transactions online is one of the reasons why people perceive Internet banking as inept to provide them the usability and security needed to convert to this mode of payment. Suh et al. [5] have identified a lack of 'trust' in security features offered by e-payment websites and third party involvement as a major deterrent of adoption to these procedures.

Khan et al. [6] has identified usability concerns related to e-payment system. Customer's perception about technology and an understanding about the system contribute greatly in propagation of a particular payment mechanism. External security threats such as theft, hacking and eavesdropping have led to failure of e-banking and e-payment system. Credit and Debit cards still have inadequate security features in its design which may be exploited easily in a country with volatile security situation.

Zugelder [7] has identified customer protection as a major issue in development of e-payment systems in countries prone to security threats. Reynolds et al. [8] have identified customers differ in the type of relationship they want to maintain with a banking network. Some would want to conduct online transactions while others would like a e-payment mechanism installed with the merchants. In counties where online transactions are extremely limited, research has to me conducted to propose a model that would address the needs of customers looking for a safe, secure point of sale e-payment mechanism. Stewart [9] claimed that customer satisfaction with banking channels in handling any misuse of e-payment systems would be an important factor in identifying the success of e-payment systems.

The study carried out by Khan et al. clearly identifies loopholes in online business environment. However, there is no focus on off-line e-payment channels that are required to provide a safe and secure alternative to cash transactions. Daras et al. [10] studied credit card security features and their impact on e-payment acceptability as a viable alternative to cash transactions. The study focuses on both online as well as offline use in POS machines. Prevention of credit card frauds has been a major security issue in dealing with e-payment transactions. The paper identifies several types of credit card frauds and attempts to propose possible solutions. Cardholder not present (CNP) frauds in one of the most widely employed card fraud that has been made possible due to development of e-commerce websites.

Appiah et al. [11] studied the electronic retail payment systems in Ghana in an attempt to delve into the user acceptability and payment problems. With an increasing number of people converging to e-payment systems, the paper attempts to discover the main usability issues in e-payment systems. The existing e-payment systems have gained overwhelming acceptance for two main reasons: convenience and reliability. When routine payments like paying electricity bills involves long queues, there is always a security risk to cash as well as loss of precious time in waiting for their turn. The research highlights the steady growth of electronic payment systems as a viable option. However, it fails to identify internal and external security threats in an online environment. Convenience of electronic payment systems in such a milieu is highlighted while usability concerns are not properly addressed.

Malek [12] and Ferguson [13] have addressed the problems of perception of technological innovations in e-payment systems. Although information technology has had a positive effect on e-payment system growth, it has left considerable security and usability problems to be solved in order to render it more effective and reliable. Humphrey et al. [14] studied that if usability and security features in present payment systems are properly addressed, it can turn supersede the conventional paper money.

Appiah et al. [11] indicate the barriers to e-payment systems in Ghana. In contrast to the convenience e-payment provides, high cost of access, lack of trust in participating parties, slack security features and lack of knowledge and skill in using these payment systems are major impediments. Moreover, low network externalities have led to limited acceptability of e-payment systems. Unless a majority of merchants do not accept a particular electronic payment system, it would not gain customer assent. An uncoordinated banking system is another reason why a unified electronic payment system cannot be formulated.

Zhang et al. [15] proposed a multiple payment system based on a mobile phone platform. They employed on card matching, fingerprint authentication and public key infrastructure on a mobile phone platform. This model addressed both security and usability factors by combining proximity security features with the portability and convenience of mobile phones. The model focuses on authentication, confidentiality, data integrity and non-repudiation issues. The design though on a mobile phone platform, is particularly suited to countries with volatile security issues and terrorism. Biometrics has been successfully employed by using fingerprint authentication.

A particular limitation to the proposed model is that it can be successfully implemented on handsets with built-in fingerprint sensors. This limitation is bound to raise accessibility and usability issues as these handsets are quite expensive. The model would only be business friendly if it is cost effective. The model takes advantage of the GSM technology by using existing SIM cards as SMART cards; an essential ingredient to making e-payments.

The provision of biometric functionality adequately ensures that the payment is being made by the legitimate user. This is a considerable improvement in credit card payments which provide security loopholes in this area.

The advantages of using this system include off-line functionality and credit card security to make transactions. The system uses a payment applet module inside the SIM card to carry out payments. A PKI based system encrypts personal information as well as credit card number. X.509 public key certificate is stored in the mobile phone. A bio-applet ensures that the SIM card information is accessed by the authorized personal only. A particular limitation to this design is that it cannot be used unless the user has a valid credit card. This facility can be employed offline at any point of sale and limits the misuse of credit cards and provides more security. The addition of biometrics has provided the added security measure absent in credit cards. Another limitation is that the technology involved is still not easily accessible and is dependent on special mobiles that support fingerprint scanning and recognition.

Ivarsson [16] explored the possibility of a mobile payment with customer controlled connection. The paper attempts to study security features in a system constructed for micro-payments in vending machines. The only connection to these machines is provided by the customer. The main advantage of such a system design is that protection against denial of service attacks as well as identity thefts.

Azami [17] constructed a similar payment system to Ivarsson's hypothetical model that constructs a payment system without a permanent connection to the vending machine with infrared communication between customer and client. A particular limitation to this technique was the supposition that every mobile phone carries an Infra red module. The customer enters a PIN code for validation and authenticity before carrying out a payment. The system does not address sufficient security features. Also, the system is not cost effective as the service providers charge heavily for the traffic propagated as result of communication between the vending machine and the user mobile via service provider. Although development of mobile payments provides convenience, security features and associated costs prevent the widespread use of such a system.

The paper evaluates the level of security in a payment system while the connection is shifted from the seller to the user mobile device. In a normal e-commerce transaction, information flow would be between the buyer as well as the seller to actualize the payment process. In this case the transaction server is controlled by the financial institution, mobile server provider or any third party. The merchant machine sends a query packet to the mobile device which routes it through to the mobile phone operator and awaits conformation. After the conformation is received, the reply packet is relayed into the merchant machine. This system although convenient does not address the possibility of an eavesdropper secretly using the PIN and using the mobile phone for such payments. Moreover, the transaction may turn out to be costly as both the financial institution as well as the mobile service provider would charge for their services. The system is more prone to malicious attacks as contemporary systems that seek double authentication.

Palaka et al. [10] presented a model for peer to peer e-commerce transactions. The system implements electronic cash based transactions in a C2B environment. The system facilitates on-line transactions in which participating financial institutions become partners. The proposed system has offered a decentralized approach to facilitating e-commerce transactions by focusing on the reliability issues of centralized payment systems offered by Internet e-commerce websites such as e-bay and Amazon. They argue that a centralized architecture though more secure, are prone to disaster amidst a single point of failure. It also poses problems of bandwidth thereby limiting their scalability.

Rehman et al. [18] proposed a viable model that adequately addresses usability and security issues in e-payment systems operating in an online environment. The paper identifies ethical issues linked with credit card payments online such as hidden charges and taxes. Moreover, leakage of private information which is used by malicious eavesdroppers while providing credit card information is also a concern. The proposed system provides a new means of online payment settlement which requires no credit cards or a bank account. The system is a fast, reliable and secure alternative to conventional e-payment methods. The easy to pay system proposes improvements in the e-commerce process as a whole rather than just focusing on design and security features of existing e-payment processes. The paper introduces the concept of an e-commerce bank. This bank would be responsible to regulate all payments made online and would authenticate as well as mediate all business transactions. One of the limitations of this design is that all merchants as well as the users would have to register with this e-bank. A very important role of such a bank would be to not only ascertain the ID of the consumer but also verify the e-commerce web-site thereby eliminating the threat of a fake web-site.

Prepaid cards issued by this bank would be used to carry out routine transactions. The system ensures that the products bought online are delivered only at the registered addresses so that it is ensured that the order is delivered to customers who have actually paid for the product. The proposed system is a plausible alternative to the conventional payment systems with added security and usability features. The paper does not address security protocols that would be used and therefore leaves a question mark on the internal security mechanism of the ETPS. Also it only addresses transactions in an online scenario. A possible extension to this model would be to propose a similar system in an offline environment.

Mandadi [20] performed a study to evaluate the relative advantages with respect to usability and security of various payment systems being used around the globe. The study focuses on anonymity, scalability and ease of use of different payment systems. Accessibility of these payment systems was also addressed.

Daras et al. [21] studied credit card security features and their impact on e-payment acceptability as a viable alternative to cash transactions. The study focuses on both online as well as offline use in POS machines. Prevention of credit card frauds has been a major security issue in dealing with e-payment transactions. The paper identifies several types of credit card frauds and attempts to propose possible solutions. Cardholder not present (CNP) frauds in one of the most widely employed card fraud that has been made possible due to development of e-commerce websites.

Wang et al. [22] identified the key limitation to this study that focuses on internal security issues only and leaves out other attributes of HCI such as usability. Another limitation is that the iKP protocol does not encrypt order information unlike the SSL protocol. The design is built on the iKP protocol can be used for both online and offline payments which is what adds to the extensibility of the proposed model. Other HCI features essential for e-payment systems are however completely ignored while placing utmost importance to security.

Renaud et al. [23] focused on the user online shopping behavior and user experience that concluded to several types of user behavior. He also discusses, why customer checkouts without buying anything in the end after adding items to their baskets. Therefore, he suggests the solution for improvement of user online shopping behavior.

In [24], authors cover somewhat different but interesting work with reference to protect the human rights of disabled persons. Authors investigate relational fundamental models to reveal the common ground of HCI technology and examine the literature for solving interaction difficulties of disabled persons especially for those with motor and visual disabilities. Somewhat related work to ours can be seen in [25-28].

3. **Human Computer Interaction-Usability and Security Concerns in E-payment Systems.**

3.1. **HCI motivation.** Design of computer systems must be tailored in consideration with ease of use, reliability and security. All these three features have to be amalgamated in order to ensure market acceptability of a software product. Cost analysis, and value based pricing are also necessary features in the design of technology products. A computer system devoid of economic viability would be of no use even if has user friendly design, and offers appropriate security. All these features are dealt with under the human computer interaction paradigm. The basic principles along which HCI is modeled include requirement analysis, conceptual design, prototyping, development and feedback for improvements.

This paper also attempts to identify loopholes in usability and security features in e-payment systems. Interface design, and access to these services to all members of a community are of particular concern. Ethical issues such as trust must also be addressed for a successful design. Lack of incorporation of trust in the design would tantamount to poor usability. Our proposed RCPS payment system attempts to resolve the issue of trust.

Human factors in e-commerce play an extremely important role in the acceptance of a technology product. Unless a product considers the intricacies of human psychology, it will not invoke assent from the users. The ever growing popularity of e-commerce as well as electronic payment systems make it inevitable to put particular emphasis on usability issues. A total customer experience would be impossible without ease of use of a computer system.

Nielson asserts the importance of proper design which would include easy interface, short response time, and reliability of a system. In a study considering e-commerce website usage, it was identified that almost fifty percent of the attempts for product access ended in failure thereby cutting the profitability of these firms by half. Unless the users are facilitated with easy to use systems that offer reliability, security and economic viability, e-commerce would not be able to earn its due share in today's corporate environment. In our bid to propose an offline e-payment system, all these HCI issues have been kept in mind so as to provide users a platform which they can trust for reliability and security.

3.2. **HCI requirements for electronic payment systems.** Considering the parameters of human computer interaction, the system must incorporate efficient design coupled with ease of use to give optimum level of user satisfaction. Technical efficiency cannot invoke user acceptance unless psychological preferences of users living under different conditions are addressed. Privacy, security, reliability, usability and scalability are all features that are coherent with principles of human computer interaction that need to be addressed. Security features must be given the highest preference as users would not feel comfortable in using a payment method that is insecure due to the decreasing socio-economic conditions in the current milieu. These parameters are elucidated hereunder.

3.2.1. *Privacy.* Anonymity is a key concern of users who transact through online means. Users would want their personal information to be protected while choosing the e-payment option. Users of credit and debit cards however have to trade-off on this feature as payments are not possible without exposing the credit card to the merchants or giving their credit card number online. Proper checks have to be in place in order to ensure privacy of the customer.

3.2.2. *Atomicity.* This is a key feature that ensures reliability of an electronic payment system. It is important to make sure that the transaction does not fail to take place. In case there is a system failure in completing the transaction, an appropriate log file must be maintained to help the system roll back to the last stable state. A delivery of an error message must be followed in such an instance.

3.2.3. *Interoperability.* This feature has been worked upon in recent years considering the real life needs to operate in different currencies and from different payment systems. Interoperability would enhance the acceptability of a payment system as it would make business transactions easier to complete.

3.2.4. *Scalability.* The system must support an increase in number of users that access the payment system.

3.2.5. *Security.* In this paper, both external and internal security threats are addressed. It is desirable that a payment system manifests itself in a way that renders it less prone to thefts, misuse and robbery. Credit cards and debit cards must have secret keys without which a thief would not be able to use the card. This issue has not been addressed in credit and debit cards. Using credit cards for online payments is still risky as any hacker can access the database of payment companies resulting in misuse the credit card. It is impossible to detect online whether the purchaser is actually the holder of the card or not. Unless these security features are looked upon, it would be impossible to replace paper money by electronic money in countries with a high security risk profile.

3.2.6. *Usability.* Ease of use is an important feature that would be an important factor in the acceptability of a payment system. Any payment system with complex features would not earn acceptability. Poor usability would lead to rejection.

In this paper we attempt to explore the usability, privacy, security and reliability features of various payment systems in use globally. We tend to highlight their weaknesses with respect to usability and security.

4. **Methodology.** Electronic payment system research takes a business perspective which involves a careful study of the competing systems in place. It is very important to delve into the strengths and weaknesses of existing systems to ensure that the proposed system offers not only better design but also provides superior security and usability. Typically, human a study of human computer interaction involves comprehensive insight to the current issues prevalent in the area of concern. We follow a similar mechanism which involves comprehensive research on the latest trends in technology as well as user perception to these evolving techniques.

A comprehensive overview of the current e-payment systems is attempted to study user perception of usability, privacy and security of the system. Unlike contemporary approach in human computer interaction literature, we have focused not only on user behavior; but attempt to link it to successful system design. We identify system weaknesses and strengths based on these behavioral attributes.

Our paper studies contemporary payment systems as well as modern literature that identify perceived usefulness of each payment system as exhibited by user behavior. The study spanned over six months of extensive research and a bid to find out user demand in a particular scenario where security threats are omnipresent. An in-depth study of previous work was carried out which resulted in the formulation of design guidelines for electronic payment systems. Existing payment systems were analyzed to formulate and validate these initial guidelines.

5. Comparison of Current Online Payment Technologies-Issues and Benefits.

5.1. **Why use an e-payment system – a country specific requirement?** Convenience and secure transactions are the hall mark of any e payment system. In the rapidly evolving business environment, customers are looking for more secure modes of settlement of day to day business transactions. Settling huge business transactions through cash is considered a cumbersome process which is no more a viable option considering the costs and security threats associated with it. Government policies are advocating strict documentation of large transactions in the economy to combat the threat of money laundering and terrorist financing. Settling business transactions through cash also involves security and maintenance related concerns.

5.2. **Macro payment systems.** Macro payment systems are designed to provide payment options for all types of payments. In general, security issues as well as usability concerns are hampering the overall acceptability of Macro payment systems. Both internal and external security threats make Macro payment methods vulnerable to exploitation. Internal security threats may arise from employees of issuing bank and hackers. External threats include thefts, loss, etc. In case a credit card is lost, the potential loss can be a lot more than in case of a person carrying cash. High transaction costs deter the use of such means thereby decreasing its convenience and eventually having a net negative impact on usability. Moreover, certain electronic funds transfer facilities such as credit cards are not easily accessible to all sections of a society in most underdeveloped countries due to credit risks involved as well as liquidity short falls. Moreover, they are not cost effective for small amounts.

6. **Usability Based Reliable and Cashless Payment System (RCPS).** The proposed system is an extrapolation of the easy to pay system as proposed by Rehman et al. [18] in an online environment. The model intends to encapsulate all the design principles listed in the Human Computer Interaction (HCI) literature. This model was proposed keeping in view various technical as well as economic limitations in developing countries. Lack of an intricate dedicated network between financial institutions has led to design alterations and involvement of a third party facilitator. The approach supports macro payments in a B2C environment.

This model is typically suited to hypermarkets which allow access to all types of consumer products under one roof. The presence of an enormous range of products provides an opportunity for customers to satisfy their periodic needs in one trip. Typically this would result in heavy spending which could be curtailed due to the limits on credit cards and the risks associated in carrying them. Internal security concerns are handled through provision of application security mechanisms. External security is ensured through provision of a proper PIN to each customer as well as through bio-mimicry (deployment of biometric authentication through fingerprint matching). Figure 2 depicts the modus operandi of the biometric applet. This biometric identification provides a double layered security. This ensures that even if an eavesdropper has secretly accessed the PIN code, he would not be able to gain access to the system due to biometric authentication. As there is no physical instrument that is needed to be carried by the customer in order to make the payment, the external security threat of theft has been eliminated.

Matyas et al. [19] have identified the usability and security features of biometric authentication. One of the major advantages of using biometric analysis is that individual

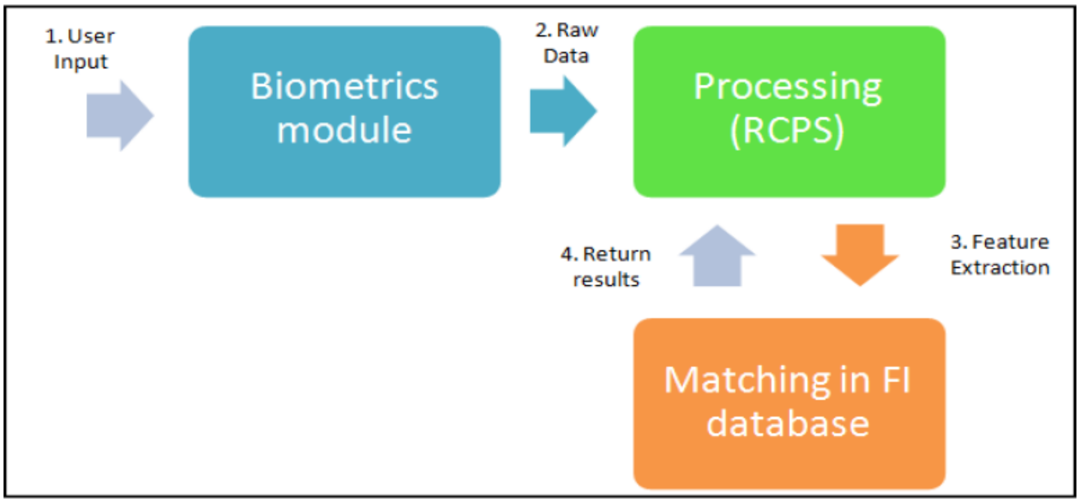

Figure 2. The biometric applet of the RCPS machine

traits such as fingerprints cannot be copied exactly. This would therefore make it almost impossible for an intruder or eavesdropper to access the account. Moreover, unlike credit cards or other mechanism deployed to ascertain authenticity, the biometric characteristics cannot be stolen. This therefore guards against the external security threats. The double check mechanism proposed in the RCPS is used to counter the false acceptance rate of one percent normally identified in such systems. This adds to the overhead of maintaining a database of PIN codes along with a trace of fingerprints but at the same time renders the system un-paralleled security.

The installed biometric applet would function in a way a normal biometric system would. The customer would access the portal after providing the relevant pin. The portal would then ask for the thumb to be placed on the input device. Both liveliness and sample quality would be verified during the process. The feature extraction module would then identify and extract features suitable for the matching algorithm and then compare it with the stored sample in the bank's database. The server then allows access to the user once the features are comparable.

The merchant would have typical barcode generator software such as Bartender installed that would convert the plaintext information provided by the authorized customer into machine readable 2-D bar code. 2-D bar code would be employed so as to accommodate more data. Typical information contained in the bar code would be the Merchant ID (account number), Customer ID, and the cost of goods. PDF417 barcodes can be read on auto scanning CCD and laser scanners. 2-D bar codes need to be deployed because of the need to incorporate more information. 1-D bar codes normally store about fifteen characters only. The information stored on the barcode slip would be given to the customer. The customer would need to carry this slip to special third party RCPS machines.

The RCPS machines would decode the machine readable code through specially installed CCD scanners after proper biometric authentication of the customer. Once this is done, the bar code sends the plain text (account number of merchant and customer to the microprocessor). The microprocessor after performing balance checks on the customer account credits the merchant account to complete the transaction. This balance check is done after the RCPS machine connects to the participating bank's server. After validation of account balance, the system confirms the successful completion of the transaction to the user. A receipt is generated that indicated the debit and credit information. The

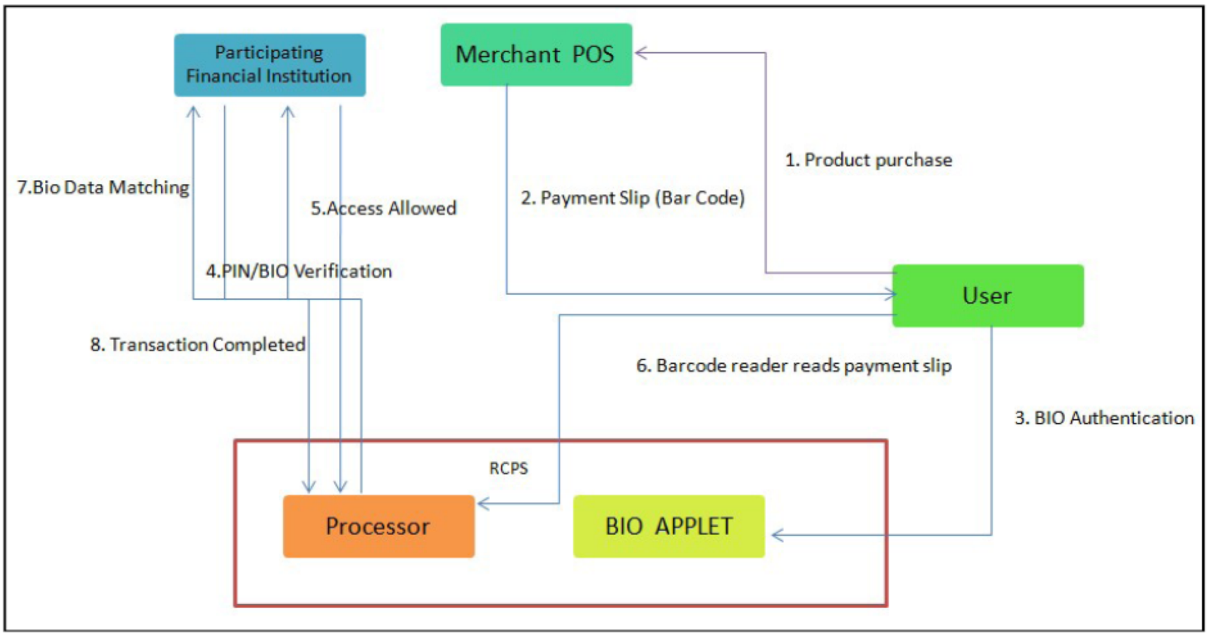

FIGURE 3. Usability based reliable and cashless payment system (RCPS)

customer takes this slip back to the merchant who can confirm execution of the transaction through the Internet banking services being provided by the participating financial institution.

Both the vendor as well as the customer would need to open accounts with the participating financial institution which shall in collaboration with a third party install RCPS machines that would allow funds transfer mechanism between the registered users of the RCPS. The machine would contain a bar code reading device as well as a biometric scanner.

Database security as well as transport layer security would be provided to cater the risks of data integrity, reliability and storage. In the security design of RCPS, various security protocols were examined. These protocols were evaluated for use on our model. Table 1 gives a gist of the various technical aspects of these protocols.

TABLE 1. A comparison of commonly employed protocols for e-payment systems

Attribute	SSL/TLS	SET (MasterCard)/iKP/Cyber Cash	CONSEPP	X9.59
		Credit Card protocol/STT (VISA)		
Security	Low	High	Modest	Modest
Usability	High	Low	High	High
Online/Offline	Online	Multi-purpose	Online	Multi-purpose

Comparison of the above mentioned protocols that the Secure Electronic Transaction (SET) protocol is the best protocol for use in an offline environment when the security level to be attained is high. Another reason why we can use the SET protocol is that it is already in use and deployed successfully by Visa and Master.

SET protocol would provide a secure mechanism of information exchange between the User and the financial institution through the RCPS system. Although the costs of implementing such a system would be comparatively high, it would ensure optimized level of security required in a system which is prone to security disruptions.

The RCPS process involves three main parties including the merchant POS system, the customer, the participating and the financial institution. The special purpose RCPS machines are provided by a third party or may be owned by the participating FI.

The proposed model provides ingenuity in that it is the only POS e-payment system that facilitates payments without the use of any physical instrument. The system eliminates the chances of unauthorized payments due to biometric safeguards in place. RCPS, unlike other POS payment systems (Credit and Debit Cards) provide an external security mechanism. It uses the already implemented SET protocols which are being used by MasterCard to bring into effect strong internal security mechanisms. The RCPS is a one of its kind in providing POS payment solutions as compared to contemporary research that offers new techniques for facilitating online payment.

7. **Conclusion and Future Work.** The Reliable and Cashless payment system offers immunity against theft of paper and e-money. It also ensures documentation of the economy through creation of transaction trail that is in coherence with the recommendations of the APG/World Bank. This provides legal protection to our model which would make it easy to implement in a real life scenario. The proposed idea in this work will be implemented via a third company especially dedicated to provide their services in this area. Furthermore the security features as well as ease of use would render it more usability and therefore customer acceptance. This design however, restricts payment settlement in a Business to Customer scenario. Future direction of research could be to formulate a system with similar features that supports person to person settlement as well. Although financial intuitions would be inclined to be partners in this business model, the provision of RCPS machines at the POS would be a challenge as it would not be possible without the collaboration of a technology giant such as Oracle or Microsoft.

REFERENCES

[1] D. Abrazhevich and M. Rauterberg, *Electronic Payment Systems: A User-Centered Perspective and Interaction Design KNAW Research Information NOD – Dutch Research Database*, 2004.

[2] D. Abrazhevich, P. Markopoulos and M. Rauterberg, Designing Internet-based payment systems: Guidelines and empirical Basis human-computer interaction, *Human-Computer Interaction*, vol.24, no.4, pp.408-443, 2009.

[3] Bruno-Britz, *Bank Systems and Technology*, International Magazine, 2006.

[4] Silva, *Customer Self Service and Retail Banking in the US: Rising Expectations, Challenges, Opportunities*, The tower group, February 2006 Ref No. V46:19NR, 2005.

[5] B. Suh and I. Han, Effect of trust on customer acceptance of Internet banking, *Electronic Commerce Research and Applications*, vol.1, no.3, pp.247-263, 2002.

[6] S. Khan, *Adoption Issues of Internet Banking in Pakistani Firms*, Master Thesis, Lulea University of Technology, 2007.

[7] M. Y. Zugeldar, T. B. Flaherty and J. B. Johnson, Legal issues associated with international Internet marketing, *International Marketing Review*, vol.17, no.3, pp.253-271, 2000.

[8] K. E. Reynoldsa and S. E. Beatty, A relationship customer typology, *Journal of Retailing*, vol.75, no.4, pp.509-523, 1999.

[9] K. J. Stewart, Transference as a means of building trust in World Wide Web sites, *Proc. of the 20th ICIS*, Charlotte, North Carolina, 1999.

[10] D. Palaka, P. Daras, K. Petridis and M. G. Strintzis, A novel peer to peer payment protocol, *Proc. of IEEE EUROCON*, vol.1, pp.2-6, 2003.

[11] A. Appiah and F. Agyemang, *Electronic Retail Payment Systems: User Acceptability and Payment Problems in Ghana*, Master Thesis, Blekinge Institute of Technology, 2006.

[12] M. Malek, *E Commerce Technologies – Electronic Payment Systems*, Stevens Institute of Technology, 2001.

[13] J. W. Ferguson, Electronic commerce, bank and payments, *The 36th Annual Conference on Bank Structure Competition*, Chicago, 2000.

[14] D. B. Humphrey, B. L. Pulley and J. M. Vesala, Cash, paper, and electronic payments: A cross-country analysis, *Journal of Money, Credit, and Banking*, vol.28, pp.914-939, 1997.

[15] Q. Zhang, J. N. B. Moita., K. Mayes and K. Markantonakis, *The Secure and Multiple Payment System Based on the Mobile Phone Platform*, Smart Card Centre Information Security Group, Royal Holloway, University of London, 2004.

[16] S. Ivarsson, *Mobile Payment with Customer Controlled Connection: Can It Be Constructed to Be Safe Enough?* Master Thesis, Blekinge Institute of Technology, 2008.

[17] S. B. Z. Azami and M. Tanabian, Automatic mobile payment on a non-connected vending machine, *Canadian Conference on Electrical and Computer Engineering*, vol.2, pp.731-734, 2004.

[18] S. U Rehman, S. Wasi and J. A. Siddiqui, Towards an easy to pay system (ETPS) for e-commerce, *International Conference on E-Business and Information System Security*, 2009.

[19] V. Matyas and Z. Riha, *Biometric Authentication, Security and Usability*, http://www.fi.muni.cz/usr/matyas/cms_matyas_riha_biometrics.pdf, 2002.

[20] R. K. Mandadi, *Comparison of Current On-Line Payment Technologies*, Master Thesis, Linköping Institute of Technology, 2006.

[21] J. Dara and L. Gundemoni, *Credit Card Security and E-Payment: Enquiry into Credit Card Fraud in E-Payment*, Master Thesis, Lulea University of Technology, 2006.

[22] H. Wang, X. Zhang and J. Sun, B2B electronic payment protocol based on iKP, *The 1st International Workshop on Education Technology and Computer Science*, vol.1, pp.1008-1011, 2009.

[23] K. Renaud, T. Cockshott and M. Hair, Everyone abandons – Eventually: Understanding the online shopping experience, *IEEE Conference on Commerce and Enterprise Computing*, 2009.

[24] F. Wang and X. Ren, A survey on human computer interaction technology for disabled persons, *International Journal of Innovative Computing, Information and Control*, vol.6, no.6, pp.2459-2467, 2010.

[25] J.-H. Yang and C.-C. Chang, An efficient fair electronic payment system based upon non-signature authenticated encryption scheme, *International Journal of Innovative Computing, Information and Control*, vol.5, no.11(A), pp.3861-3873, 2009.

[26] G. Liu and Y. Zhou, Transportation cost payment problem in a two-echelon decentralized supply chain, *ICIC Express Letters*, vol.4, no.2, pp.427-433, 2010.

[27] J.-H. Yang and C.-C. Chang, An efficient payment scheme by using electronic bill of lading, *International Journal of Innovative Computing, Information and Control*, vol.6, no.4, pp.1773-1779, 2010.

[28] W.-G. Shieh and W.-B. Horng, Security analysis and improvement of the remote user authentication scheme without using smart cards, *ICIC Express Letters*, vol.4, no.6(B), pp.2431-2436, 2010.