China-USA Business Review, Oct. 2017, Vol. 16, No. 10, 491-503
doi: 10.17265/1537-1514/2017.10.004

Design and Simulation of NFC-Based M2M Payment Model for Mobile Phone With Trusted Platform Module

Chinyere Grace Kennedy, DongSub Cho
Ewha Womans University, Seoul, South Korea

The introduction of the information technology (IT) plus the introduction of the internet, has been said to be the source of advancement in electronic commerce. It's focused on that, in the future, predictably, the society will be cashless, the circulation of physical cash will have decreased. The use of IT especially in the finance and industrial sector, not forgetting the proliferation of ecommerce hasled to increased speed in arising of electronic cash. The use of cashless methods, is appealing to the younger people. This is the reason why machine to machine (M2M) is gaining momentum as days go by. Some countries like Korea, implementation of cashless money methods, the electronic cash has been on a steady rise since 2000. A good example is the T-Money transport card. This is prepaid or postpaid electronic cash. It is very popular transportation card, which is widely used throughout most parts of Korea. In the future, its use will most likely to be expanded if it becomes integrated T-Money. The postpaid T-Money is a good example of M2M implementation, in which users now don't need to carry cash to travel. They can transfer the money from mobile phones to the billing systems in the transport vehicles seamlessly. The transport card has developed into a mobile payment system in recent years and has become increasingly popular in Korea. This research paper, will focus on the design and simulation of machine to machine using NFC-based payment model. This will mainly target smartphone applications, which are more popular nowadays, not only amongst the youth but all generations.

Keywords: NFC payment, machine to machine (M2M), cashless money transfer, electronic cash, mobile money

Introduction

Nowadays, many types of computing devices (e.g. personal computer, server, personal digital assistant, printer, mobile tablet, or a mobile phone) are increasingly being used for both business and personal purposes which involve use of sensitive data (Arthur, Challener, & Goldman, 2015). Examples of these include: e-commerce services, online banking, e-health, e-government services etc. Thus, there is growing need to make these computing platforms more secure and trustworthy. Modern cryptography, information security, and internet security protocols provide diverse types of security measures. However, these measures are not completely dependable if the underlying computing platforms (hardware and software components) have security flaws. In communication, endpoint devices are easier targets to compromise since they are

Chinyere Grace Kennedy, Ph.D. candidate, Dept. of Computer Science and Engineering, Ewha Womans University, Seoul, South Korea.
DongSub Cho, professor, Dept. of Computer Science and Engineering, Ewha Womans University, Seoul, South Korea.
Correspondence Concerning this paper should be addressed to Chinyere Grace Kennedy, Dept. of Computer Science and Engineering, Ewha Womans University, Seoul 120-750, South Korea.

usually more vulnerable to attacks by malwares. To combat this vulnerability, the TCG has initiated a set of provisions to generate a computer system with advanced security called Trusted Platform (TP) (Le & Bouzefrane, 2014).

> Trusted platforms have been proposed as a promising framework to enhance the security of general-purpose computing systems. However, for many resource-constrained embedded systems, the size and cost overheads of a separate Trusted Platform Module (TPM) chip are not acceptable. One alternative method is to use a software-based TPM, which implements TPM functions using software that executes in a protected execution domain on the embedded processor itself. However, many embedded systems have limited processing capabilities and are battery-powered; it is also important to ensure that the computational and energy requirements for SW-TPMs are acceptable. (Aaraj, Raghunathan, & Jha, 2008, p. 2)

The TP, otherwise known as TPM is usually executed at a chip level. One of the goals of this "architecture is to improve the security and the trustworthiness of computing platform (both hardware and software)" (Aaraj et al., 2008). There are two key components related to the TP. These are shielded memory locations and protected capabilities. Most TPM chips have crypto processor architecture, which makes it typically hardware-based (Arthur et al., 2015).

As a hardware-based platform, the TPM is extremely expensive and therefore advisable to implement as software-based as it provides easier and cost effective option to incorporate into an e-commerce platform.

The TCG has introduced TPM as the most appropriate solution in ensuring confidentiality and privacy in computing systems. Many users and systems, where protected storage is concerned, mandate TPM to be their "root of trust" (Le & Bouzefrane, 2014). Hence access is only within TPM as it acts to shield computers from unauthorized access by unwanted users (Le & Bouzefrane, 2014). It is noteworthy that the design of TPM is such that it prevents attacks on software attacks with marginal consideration on physical attacks. Thus, the focus of TPM is the PIN (Personal Identification Number) identification to govern the user's physical presence. However, the PIN password method does not qualify as the best method for user verification.

Some researchers (Kuntze, Rudolph, Bente, Vieweg, & Helden, 2011) show that a substantial number of vulnerabilities, both known and unknown to the client can alter the industrial software practices. Majority of threats that affect computing systems do so through servers and networks because users are not keen to update the patches due to time consuming. A compromised client's information may be available to the user through the TPM that has been supported, thereby preventing attackers. TPM is enabled by the network administrator to work actively to prevent compromised clients. TPM provides secure barrier which enables the client and the server to communicate without endangering sensitive information including networks they might be connected to. To lessen the vulnerabilities rate in software, the client is compromised for the protecting sensitive information and confines the damage through seeking the recognition of TPM.

The paper is organized as follows: Introduction—which gives a brief introduction of TPM and definition of terms; Related work—which mirrors existing literature on the implementation of TPM on e-commerce; design the access control-based architectural framework for implementation of secured TPM on e-commerce; the design objectives and scope ofexperimental expectation; highlighting a software simulation example that can be used with the TPM; and the conclusion.

Related Work

E-commerce implemented on TPM provides some level of security however there is no 100% protection

against attacks therefore it is necessary to give additional security measures to the underlying computing platform. For this reason, several researches have been conducted to further enhance the security and trustworthiness of TPM and the sensitive applications that run on them.

Accroding to Aaraj et al. (2008), it was discovered that TPM has some weaknesses in integrity measurement features, which are susceptible to attacks like software attack, timing attack, and reset attack. These attacks were tested on TPM using various PC platforms such as Linux, IBM, and Windows. And the results indicated that trusted platform does not always mean to be trustworthy as many OSs and BIOSs have security holes. The experiment also checked how well TPM can securely store keys. For further protection on a system with TPM, it was proposed in this experiment that a memory that cannot be modified by any attack should be used as defence against software attack, while secure bootloader should be used to rectify reset attack since it mostly involved the BIOS and RSA binding for timing attack.

In the Trusted Computing Group(TCG, 2016), problems are related to the availability and management of sealed data with respect to software update and hardware migration, which cause obstacles to trusted computing such as e-commerce applications. TPM makes sealed data inaccessible especially when intrusion is detected or during update or security patch, however these sealed data could be needed to properly execute such programs. TPM migration to TPM or other platform makes use of enormous amount of certificate and traffic and there is no guarantee of the security and availability of TPM services after migration. The authors (Jacques Benoit, 2006; Kruntze, Bessane, Feitosa, & Cunha, 2014) proposed software solution to provide multilayer security and decentralized control that allow only authorized parties/trusted parties to:

> Help to mediate between the interests of the involved parties, without a central authority like the TCG prescribing a trusted party. Furthermore, this principle protects the privacy of a system's owner and user as well as the security interests of remote parties.

"In our paper performance evaluation of the energy and execution time overheads for a SW-TPM implementation on a handheld appliance" (B. Ballad, T. Ballad, & Banks, 2011). This paper characterizes the execution time and energy required by each TPM command through actual measurements on the target platform. This paper also observes that for most commands, overheads are primarily due to the use of 2,048-bit RSA operations that are performed within the SW-TPM. To alleviate SW-TPM overheads, it then, evaluates the use of Elliptic Curve Cryptography (ECC) as a replacement for the RSA algorithm specified in the Trusted Computing Group (TCG, 2016) standards. In addition, the authors also evaluate the overheads of using the SW-TPM in the context of various end applications, including trusted boot of the Linux operating system, a secure VoIP client, and a secure Web browser. Furthermore, the authors analyse the computational workload involved in running SW-TPM commands using ECC. The authors then present a suite of hardware and software enhancements to accelerate these commands—generic custom instructions and exploitation of parallel processing capabilities in multiprocessor systems-on-chips (SoCs). The authors report results of evaluating the proposed architectures on a commercial embedded processor, "through uniprocessor and multiprocessor optimizations we could achieve speed-ups of up to 5.71X for individual TPM commands" (Aaraj et al., 2008).

E-commerce

E-commerce (electronic commerce) refers to the business transactions conducted via an electronic network i.e. mainly the internet (Daniel, 2011). Such operations include transmission of data/funds and purchasing and selling of goods and services. These can occur within businesses, between business-to-consumer or

business-to-business interactions. The e-commerce is interchangeably used with e-business (electronic business) though there are slight differences. While e-commerce is a description for business transactions over the internet, e-business entails the necessary re-designing of a business enterprise into a networked business model that is grounded on the web (Daniel, 2011).

The e-commerce has a long history dating back to the 1960s when the electronic data interchange (EDI) began to gain prominence in businesses for the sharing of documents with other firms. It has therefore continued to grow especially in the American markets, and this is sparked by the sustained rapid advancements of technology. This ensures speedy access to and greater availability of products and services, round-the-clock availability, ease of accessibility, and global reach. For security, privacy, and effectiveness purposes, businesses are advised to authenticate their transactions, control access, and encrypt their communications (Aaraj et al., 2008).

Trusted Platform Module

The continuous increase of computer users and connections between computer systems has generated more need to be protected from attacks. TPM is a computer chip that is designed for the safe storage of artefacts, like passwords and encryption keys, which are used in the authentication of platform i.e. a laptop, mobile phones, PC, or networked equipment (Arthur et al., 2015). It can also be used for keeping platform measurements for the maintenance of its trustworthiness. The TPM chips have a pair of RSA keys which are inwardly maintained to ensure protection against any external software attack. Various applications for TPM secret storing can be formulated to prevent unauthorized access to information on computing devices in case the devices are stolen (IBP, 2016). The chips can efficiently and successfully be used with any operating system alongside security software such as antivirus software and firewalls.

TCG (2016) principally offers TPM of various cryptographic capabilities, which assist in protecting the users' sensitive information and computers from threats. The group designed TPM to have specifications of microcontroller with security features (as seen in Figure 1). In its capacity as a microcontroller, TPM contains security features, including digital certificates, passwords, and keys "non-bulk RSA encryption and decryption, Hash function, protect and securely store cryptographic keys (and other credentials), and pseudo random number generation." (Chin & Older, 2011). Meanwhile, as a hardware resource, TCG states TPM as the core to scheme many applications to offer more "root to trust". TPM provides a safe environment to store sensitive information and to secure key operations. The security for crucial tasks is also performed by TPM to give a report on integrity measurement. To heighten platform security, a specially designed software-based attack, software information and software key has been demonstrated. To protect against potential damage that may arise from various threats and attacks, there has been a TPM that has been designed.

The TPM can be used alongside other software such as firewalls and antivirus. Hence the example of a program/software that can be utilized with TPM on e-commerce is the Microsoft BitLocker. This program encrypts the boot volume of a computer/computing system and shields the data as well as the operating system, windows registry, impermanent files, and hibernation file (Ballad et al., 2011). Therefore, with TPM, the BitLocker locks the encryption keys as it protects the stored data. As such, no access can be allowed to the keys until verification by the TPM concerning the state of the computer as it boots.

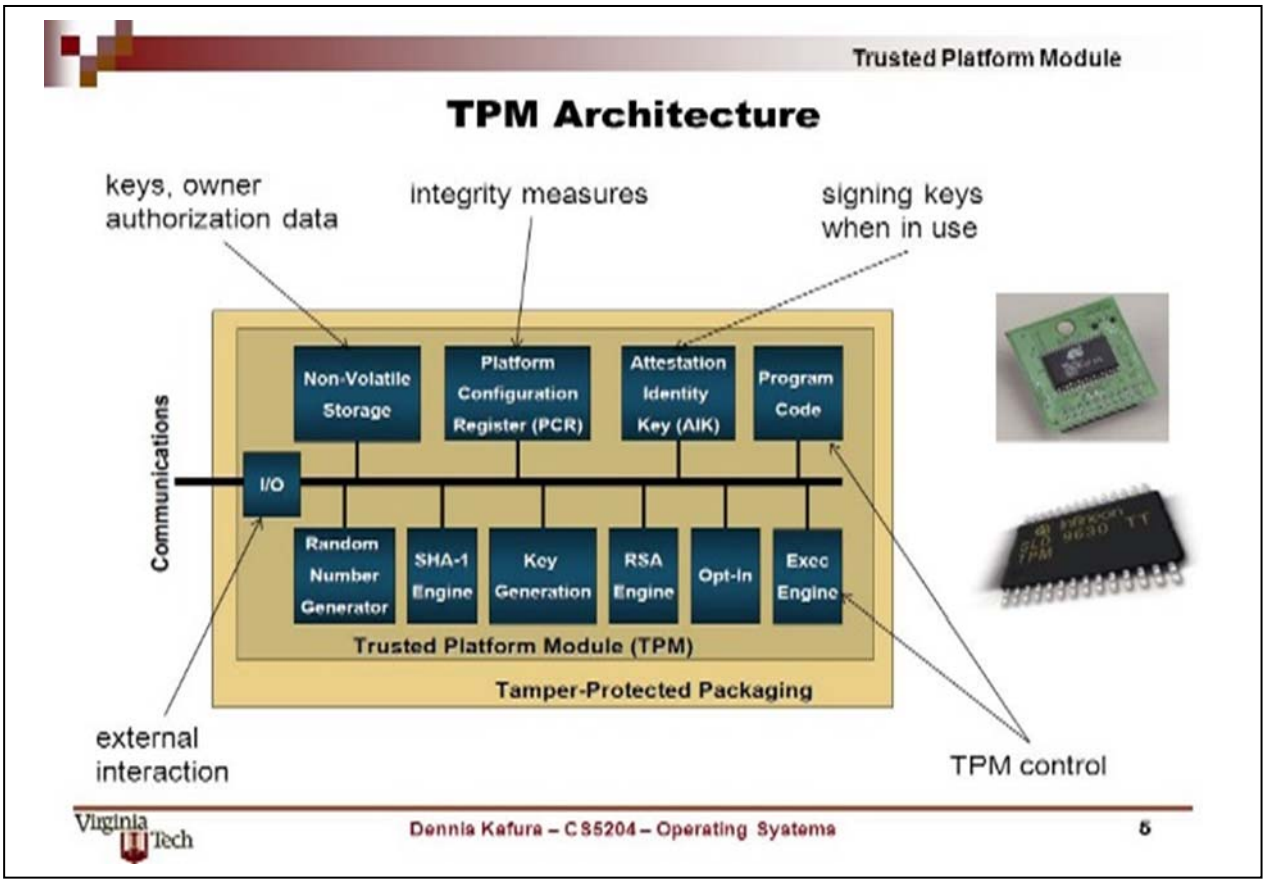

Figure 1. TPM architecture (Arthur et al., 2015).

Access Control-Based Architectural Framework

Existing security systems have a natural fault in that they override the unknown hardware. However, systems containing TPM store sensitive information on a different piece of hardware in place of a safe location. The TPM chip distinctively identifies this hardware and disallows sensitive data (e.g. keys) to leave the TPM. It is impossible to access the sensitive data directly outside of TPM, whose hardware is designed to shield sensitive information from being stolen physically. The designed hardware is not as valuable as information that has been stolen from the client system. The physical meddling is not needed to safeguard the data while using TPM.

Additionally, network security is essential in today's life. Chaudhry, Naqvi, Sher, Farash, and Hassan (2015) agreed that many times secret information is hacked into by unauthorised persons who may not even have access from the server. This hacking can be evaded using methods such as decryption, encryption among others. Still, some hackers can infiltrate information brilliantly without hacking the security systems. To avoid such happenings, it is imperative to institute a methodology that has new authentication procedures, which can aid in providing security between client and server. In this regard, only the approved client can have access to data from the server, while any other unauthorised person is restricted. Hence, the use of TPM stands out as the most appropriate methodology for a secure authentication system.

There are several basic features that a trusted platform should always have (Chaudhry et al., 2015). These include protected capabilities, which are a sequence of commands that have special authorisation to access

locations that have been protected like registers and memory. Other features include reporting and storage, integrity measurement, machine attestation, machine authentication, and data protection in which the TPM offers a whole set of apparatuses used in safeguarding authentication—see Figure 2. For TPM to be implemented successfully, the application must be based on transferring security into hardware. In aspect of integrity measurements, the metrics of the platform characteristics are taken, and later they summarised and presented reporting and storage features.

When TPM detects intrusion correctly, then the sensitive information will not be accessible to the attacker. The sensitive information of each shared client using TPM in an environment facilitating multiple users is protected. Secret information from the client to client cannot be accessed by either using such permissions. The TPM is a security module that is cheap and which delivers the basis for a safe computing environment. Trusted computing enables users to measure the trustworthiness of the computers that they relate with and create a basis for software processes dependence. The TCG describes trusted computing as an apparatus that acts in a specific manner for a reason. The main objective of the TPM is to offer this assurance to the users relating to the client and the client themselves. Additionally, TPM has an Attestation Identity Key (AIK) which shields a device against illegal firmware and software alteration. It is worth noting that attestation or any TPM functionality does not convey personal information of a platform user. These features enhance security in numerous computing instances such as in e-commerce and online banking.

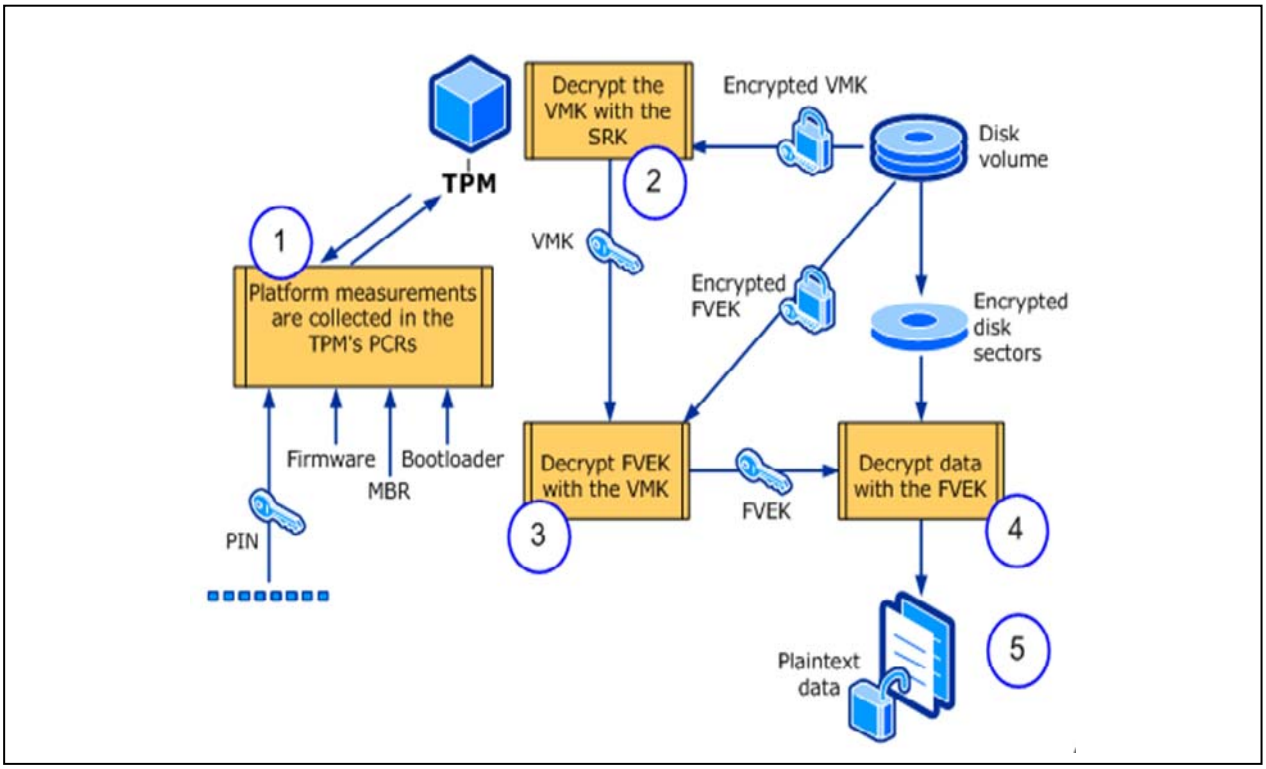

Figure 2. Sensitive features of TPM (Le & Bouzefrane, 2014).

However, the TPM does not control the software which runs on the platforms. This is because it only keeps pre-run-time configuration commands but the policies linked with the stored information are determined and executed by other applications i.e. subjects (TGC, 2016).

Access Control-BasedArchitectural Framework for Implementation of Secured TPM On E-commerce

Access control is a security procedure that governs the viewing or using of resources/information within a computing set up (Nahari & Krutz, 2011). Access is the interaction ability of subjects and objects. Therefore, access control involves coming up with rules and regulations for granting permission, rights, and privileges for interaction. In other words, it precisely outlines who intermingles with what, and what can be done by a subject in the process of interaction. The components of access control are policies, subjects, and objects. There are also access control systems which are made up of the following elements i.e. procedures, policies, and tools (Chaudhry et al., 2015).

The access control subjects are the human beings or other applications which seek for access to a resource like a file system, network, or a printer (Nahari & Krutz, 2011). They are categorized as authorized, unauthorized, and unknown subjects. The authorized subjects are those with valid and approved credentials for access while the unauthorized lack the right credentials or proper privilege for access. On the other hand, the unknown subjects are those with totally no credentials and it is not known whether they deserve access or not. The distinction between unauthorized and unknown subject is the timing i.e. unauthorized person has attempted to gain entry while an unknown one has not tried. Broadly, technology offers four primary subjects for access control, and these are systems, applications, networks, and processes (Nahari & Krutz, 2011).

Hence the access control based architectural framework for implementation of secured TPM on e-commerce will involve three primary procedures.

Objectives and Scope of Expectation of Implementing Secured TPM on E-commerce

Implementing a secure TPM for electronic commerce can fulfil the following objectives. First, it is aimed at achieving the greater level of security while transacting business online. This is realized by limiting access to the authorized users only. Secondly, it is to improve the customers experience as they shop and enhance accessibility to clients and businesses globally. Further objective of implementing secured TPM on e-commerce is to operate high-frequency business activities (Khosrow, 2015). Moreover, the scope of expectation is supporting an increased system transaction and modification for software and control systems to transcend the corporate domains (Yuan, 2015; Kreutz, Bessani, Feitosa, & Cunha, 2014).

Proposed Methodology to Develop the Software Simulation Modules

The iteration and increment follows the standard waterfall model with the difference that it loops through each level to ensure its completion (Manzoor, 2010). The main reason for selecting this model is its flexibility with changes on any level in the development process, which makes it easier to make any correction or changes on any level to add functionality or make any corrections.

One of the downsides is the time required to iterate through completed levels of the development process. When trying to minimize this there was more focus on the requirements analysis to ensure that all requirements were taken into consideration.

Development process includes four levels (Figure 3):

Requirements & Analysis Level: This initial stage of the development process involves the gathering and analysis of the user and the system requirements. This justification for this project is given by the fact that the access control based architectural framework has no other visual modelling tool. The scope and boundaries of

the project were given by the user analysis and architectural framework requirements. The system requirements were realized by understanding the framework and analysing its constraints and behaviours.

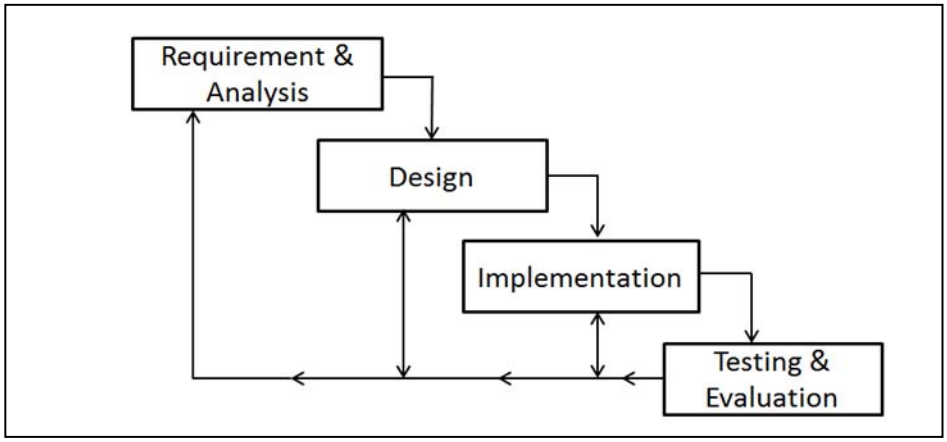

Figure 3. Waterfall workflow design method.

Design: This design phase of the framework focuses on the design of the application architecture. Due to the size of this development phase a rather significant approach was applied to maximize the limited amount of time.

Implementation: This phase of the lifecycle model involves the actual implementation of the application using programming language. In the cause of design, several problems and decisions were reached during the implementation process and documented.

Evaluation & Testing: This final phase of the lifecycle is to test functionality of the completed application and evaluation to what extent it has met user and system requirements.

Result: As mentioned above this project follows an iterative and incremental lifecycle of the simple waterfall model that includes the four phases from requirement analysis to evaluation and testing. After gathering the requirements and modelling, then the design was done with a chosen architecture and implantation followed directly into the testing and evaluation of the complete application.

Analysis of Transactional Information

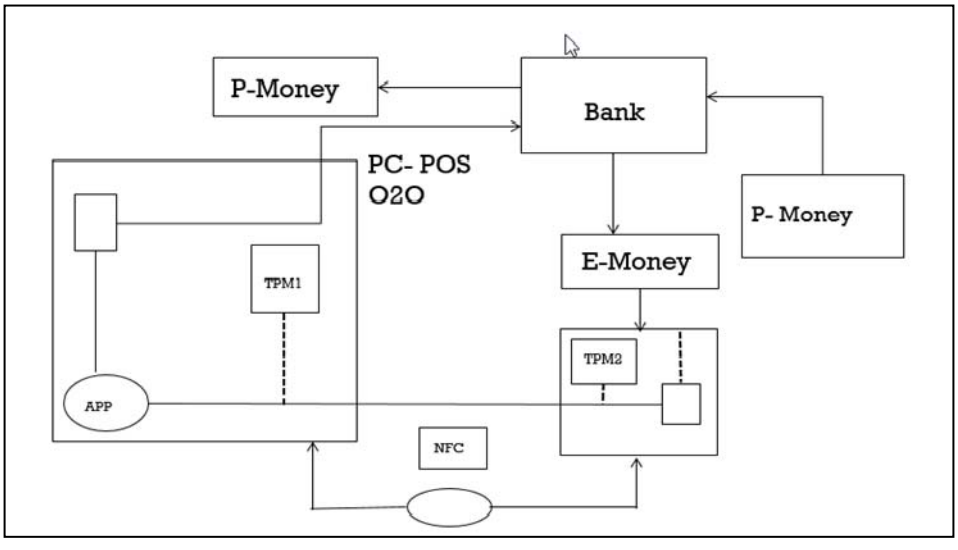

Figure 4. Our core architecture.

TPM initiates trust for valid user and safeguards the information as well as blocking the information from unapproved users and uninvited access. The method has a known record of good performance in safeguarding data and has been experimentally substantiated in numerous organisations such as banks, IT companies and so on. The method implements (Wikipedia, 2015) its projected algorithm in Net by concealing background application from uninvited access. The implementation does well and fulfils the aim of the project by offering security among the data. As in our architecture above in Figure 4 the process approach is to secure a transaction using TPM. The paper money and electronics money is safeguarded through this process. The communications between the end user and the device are authenticated using user identity which could be biometrical information, sharing of secret such as PIN, password, or key and an object such as smartphone or smart card. With data integrity which TPM offers precision and validity are maintained.

In the banking sector, each employee is assigned a task and given a different apparatus. On implementation of the software, when the machine is being entered for the first time, the connection is run from the background by the service. This takes place between the server and the client, gathers the data and is then processed per the algorithm. The data that have been processed can then be saved to the server. For every moment, the bank employee enters the system, there is automatic verification on the information relayed where after the employee is then permitted to access the system. In instances where verification fails, the employee is automatically blocked from accessing the system. Hence, sensitive information like currency details, transaction details, and customer information is all protected using the proposed (Wikipedia, 2015). This restricts users who aren't logged in as members from accessing shopping carts product or purchasing the product without authorization. The access control enables the website to track movement of customers from one page to another and allows selected users to access certain pages.

Figure 5. Administration screen page.

The system section includes all the graphical user interface elements such as dialog boxes and main menu view of the application, where system administrator will click on any of the buttons and check necessary transactions as in Figure 5. For the case of error, user is informed of the error basically if data are entered for any credit card in error and the button is pressed to check. When error is observed then the system administrator will click on those messages to send back (Figure 5) an error message to the customer.

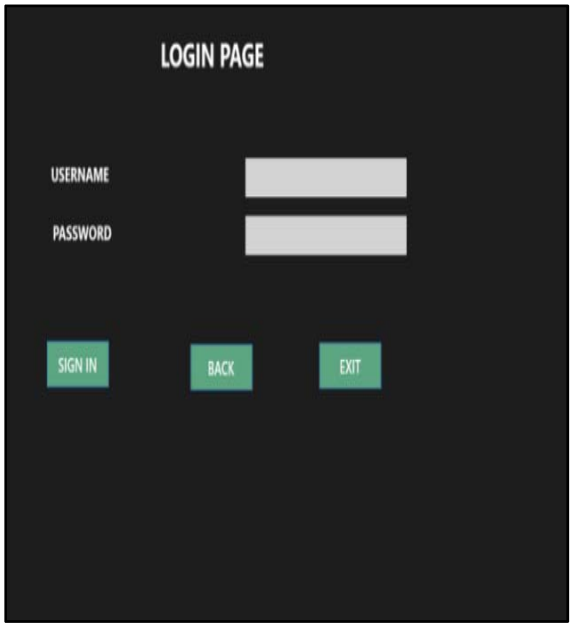

Figure 6. Login screen page for identification and authentication.

This section includes the login parameters of administrator per time in Figure 6. If the user inputs the correct username and password, then he can be authenticated and allowed to access the site by the key generated by TPM. The login parameters have been assigned to each system administrator that will login at different times. The administrator having linked to the IP address will login to have access to all the transactions made of the IP address. The exit button is close if not ready to access the message, and press back button to move back to check the IP address.

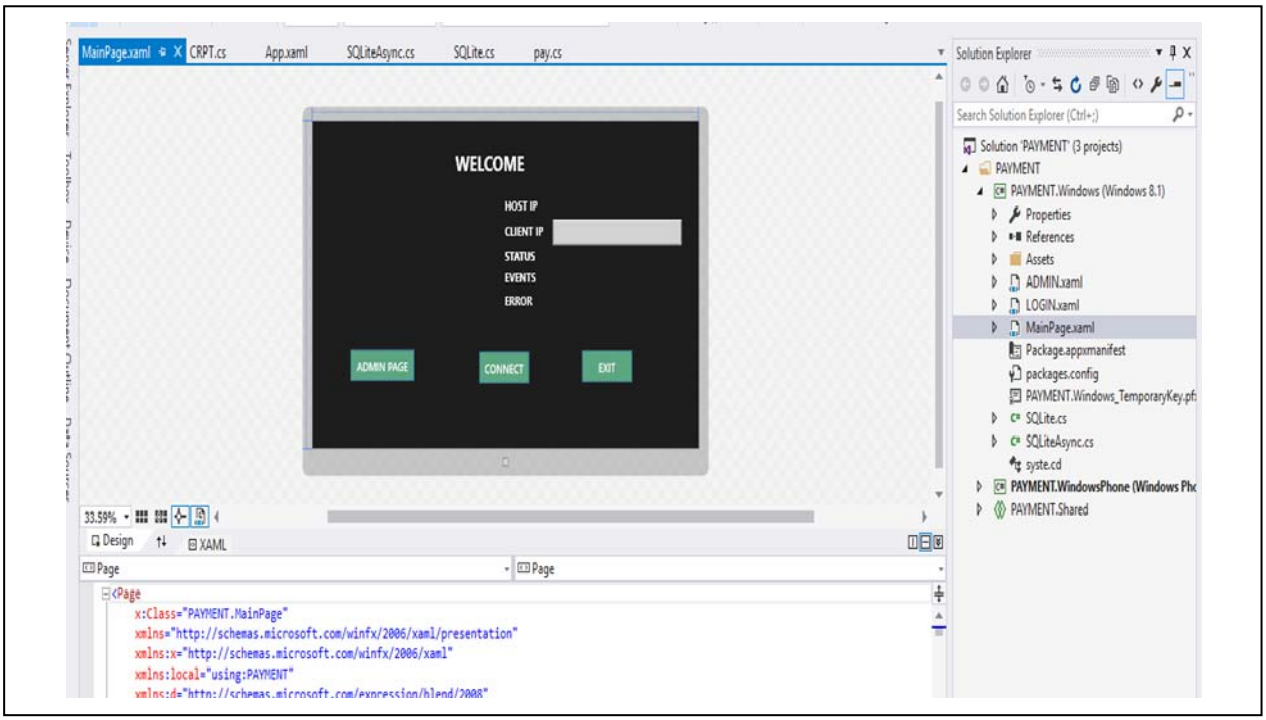

Figure 7. Welcoming screen page.

This section includes the entry of the IP address to logon to the app database linking to the system Administrator side of the server. This section when linked will enable administrator sees all transactions made as in Figure 7.

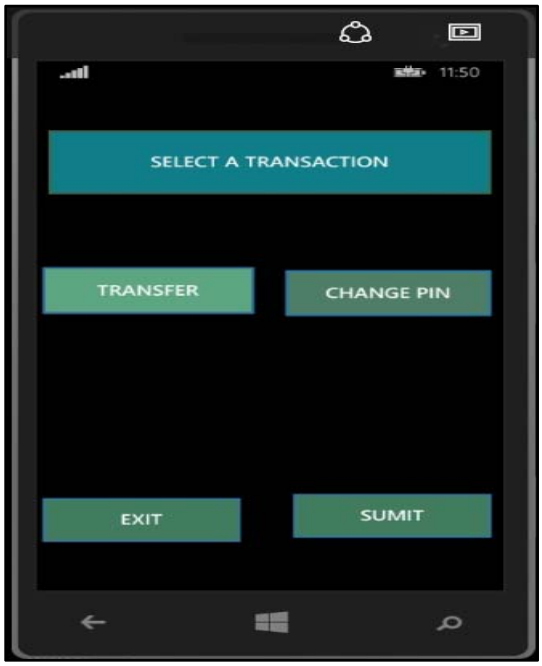

Figure 8. Screen page for displaying phone interface.

This section enables the client or customer to access the application and open to make a transaction with mobile phone shown in Figure 8. On this page, the kind of transaction will be specified and the kind of transfer or payment mode will be selected. Included on the page is the exit if the customer is not sure of what to be done or submits the transaction after making due selection of the transaction and payment mode.

Figure 9. Credit card screen page.

In Figure 9, if the user inputs the correct username and password, then he can be authenticated and allowed to access the site by the key generated by TPM section including the select of the payment on the credit card details which will be encrypted via TPM for sending a mail to the administrator of the transaction made and the payment when link to the customer's bank will confirm payments or proceed to confirm details. At the system end if the submit button is clicked, an email and success in payment will be sent to the administrator to conclude the transaction. Cancelling button makes the customer start over when they are ready to make payments.

Figure 10. Screen page after successful payment process.

In Figure 10, if the required details are incorrect, the users will be notified and prompted to enter the right password or to acquire authorization to access the e-commerce site. Users who log in successfully can view the products displayed on the site section stating the conclusion of the transaction at the client or customer end.

Conclusion

This paper has designed access control-based framework for the implementation of secured TPM on e-commerce. TPM is a computer chip that is designed for the safe storage of artifacts such as passwords and encryption keys. It is used to authenticate platform such a laptop, mobile phones, PC, or networked equipment. Access control refers to any security procedure that regulates how information/resources in a computing environment can be viewed or used. In implementing access control based architectural framework for a secured TPM on e-commerce involves three main stages: identification, authentication, and authorization. The objectives of the implementation include achieving the greater level of security, improving customers' shopping experience, and the scope expectation is supporting an increased system transaction, modification for software and control systems to transcend the corporate domains. All the programs used in this paper are coded by C# programming language. So practical enhancement would be possible by adding more detailed functional modules.

References

Aaraj, N., Raghunathan, A., & Jha, N. (2008). Analysis and design of a hardware/software trusted platform module for embedded systems. *ACM Transactions on Embedded Computing Systems* (TECS), *8*(1), December.

Arthur, W., Challener, D., & Goldman, K. (2015). *A practical guide to TPM 2.0: Using the new trusted platform module in the new age of security*. Berkely, CA: Apress.

Ballad, B., Ballad, T., & Banks, K. (2011). *Access control, authentication, and public key infrastructure*. Sudbury, MA: Jones & Bartlett Learning.

Chaudhry, S. A., Naqvi, H., Sher, M., Farash, M. S., & Hassan, M. U. (2015). An improved and provably secure privacy preservingauthentication protocol for SIP. Business Media, New York, USA, *Peer-to-Peer Networking and Applications*, *10*(1), 1-15.

Chin, S. K., & Older, S. B. (2011). *Access control, security, and trust: A logical approach*. London: CRC Press.

Daniel, I. (2011). *E-commerce: Get it right* (1st ed.). Neuro Digital.

IBP. (2016). *US e-commerce business guide: Volume 1: Strategic, practical information, regulations*. Washington, D.C., USA: International Business Publications.

Jacques Benoit, J. L. P. (2006). Making the most of substation IEDs in a secure, NERC compliant manner.

Khosrow-P, M. (2015). *Strategic e-commerce systems and tools for competing in the digital market place*. Hershey, PA: Business Science Reference.

Kuntze, N., Rudolph, C., Bente, I., Vieweg, J., & Helden, J. (2011). Interoperable device identification in smart-grid environments. *IEEE Power and Energy Society General Meeting*.

Kreutz, D., Bessani, A., Feitosa, E., & Cunha, H. (2014). Towards secure and dependable authentication andauthorization infrastructures.

Le, T., & Bouzefrane, S. (2014). Trusted platforms to secure mobile cloud computing. *The 16th IEEE International Conference on High Performance Computing and Communications*, Paris, France.

Manzoor, A. (2010). *E-commerce: An introduction*. Saarbrucken: LAP Lambert Acad. Publishers.

Nahari, H., & Krutz, R. (2011). *Web commerce security: Design and development*. Indianapolis, IN: Wiley Publishing.

Siti, H., Nor, A., & Jalil, A. (2011). The impact of non-farm income on the incidence of poverty among farmers in Kedah, Malaysia. *IJTEF*, *2*(4), 326-330.

Yuan, T. (2015). Lecture 5: High level design, presented for the software. Engineering Module, Computer Science Department, University of York.

http://www.trustedcomputinggroup.org/trusted-platform-module-tpm-summary, January, 2016.

https://en.wikipedia.org/wiki/Trusted_Platform_Module, July, 2015.