IJMTST

Volume: 2 | Issue: 04 | April 2016 | ISSN: 2455-3778

A Secure and Robust Cloud-based Prototype for Online Transaction using Android Mobile Devices

Ms. Lavanya G

Department of CS&E, P.E.S College of Engineering, Mandya, Karnataka, India.

ABSTRACT

The current scenario of mobile application based payment processes requires web or mobile channel which can be applicable for authenticating the identity of a remote user. Most of the current activities such as online banking, online shopping, etc. are configured with mobile devices. Since the applicability of m-commerce included various financial transactions along with personal details sharing, therefore, the vulnerability of performing attacks and threats by users have increased. The current research trend highlights that multi-factorial authentication techniques can be reinstalled on other devices, for overcoming this situation. This study introduces an android application based multi-level security model which is very lightweight, user-friendly, and distributed application to overcome the security issues in m-commerce platforms. Each module is made up of several supportive modules performing various operations and contributing to the performance enhancement of the proposed system. The performance evaluation of the proposed system ensures cost effectiveness regarding resource allocation and highly secure environment for online transactions using a trusted third party.

KEYWORDS: *Android, Cloud Architecture, M-Commerce, Security, Trusted Third Party (TTP).*

I. Introduction

The utilization of Mobile Commerce is quickly expanding. The use of Mobile devices is not confined to call, writings or for mixed media. With the expansion in the utilization of Smartphone which postures enhanced memory, quicker processor, and bigger screen made it easy for the client in utilizing different applications. Portable trade, in general, implies performing online exchange using small gadgets like hand-held PCs, advanced smart phones or tablets. These remote devices will collaborate with the cloud-based system which gives the capacity to conduct online purchase through merchandise modules. Any monetary exchange is considered as E-business exchange. Mobile commerce trade is considered as one of the subclasses of E-Commerce business.

E-Commerce business also can be additionally called as Mobile Commerce trade [1]. The customer's social movement from retail shopping to retail shopping has given a chance to the remote electronic gadget makers. Portable electronic business is another intends to buy online things from online stores or electronic storefronts from computerized administration suppliers. Cloud intervened system encourages the exchange process through electronic store seeks and electronic purpose of offer abilities. The youthful era is the principle focus of the gadget sellers since they widely utilize the cell telephones more contrasted with another age bunch. Inciting the coordinated effort of online merchants with huge names in telecom industry keeping in mind, the end goal to advance the progression of e-business to m-trade such that the purchaser can perform shopping through his mobile [2] [3]. The advancement associated with mobile commerce is accomplished through complex application outlines which are always rising and developing.

As in each innovation, even m-commerce business applications are inclined to security threats running from Passive stealthily into other's message so as to steal client's information. This

can hurt the customer as they are worried about their information being gotten to wrongfully. Another issue connected with m-commerce is danger included in data exchange over the systems. This issue constitutes two sections: recognizable proof trustworthiness and message integrity. Identifiable proof integrity applies to find out components present in the signal with a particular end goal to build up the root of a message. Message trustworthiness or message integrity alludes to subtle elements in building up the word got assent and guaranteeing no change or adjustment is endeavored by any evil outsider [4].

Now a day's Mobile phones have become so necessary in the field of business and commerce where a vast amount of transaction details associated with Personal Identification Number (PIN), Bank Account Number (BAN), etc. are transmitting through a network which consequences modification of data by some intruders. Mobile commerce has a need for securing the personal as well as transaction information to provide a secure mobile payment. The current research trends highlight that existing network security protocols are not sufficient to mitigate the issues associated with the user authentication, modification of data and data transferring. It can be seen that authentication of a user using a mobile device is not so easy; therefore using a mobile-based banking application one may compromise his/her security details with the intruders. For mitigating the issues mentioned above a secure, lightweight and powerful Android based mobile application has to be developed to increase the usability and trustworthiness of the mobile based online payment services.

The paper is organized as follows Section II discusses the recent studies towards energy efficient digital distortion techniques which are followed by problem statement in Section III. Section IV discusses proposed system followed by a discussion of algorithm implementation in Section V. Section VI presents the result analysis followed by conclusion in Section VII.

II. RELATED WORK

This section introduces various states of art studies towards mobile based user authentication mechanisms configured with both customers as well as merchant bank accounts. This section discusses various m-commerce based authentication mechanisms which carried out on recent work and study of standard authentication protocols in M-commerce services.

The study of [5] investigated driving of 2 variable confirmation programs that join both security and accommodation utilizing QR (Quick Response) code with advanced mobile phone clients can login to the site without to put 6 to 8 digit codes, for example, OTP (One Time Password). Customers can appreciate the both security and accommodation. They empower further research into mechanical improvement inside of web security frameworks given the critical part security structures play in the development of online markets.

The investigation of [6] introduced a reliable confirmation system that adventures the utilization of cell phones to give a two-variable validation technique. Their methodology utilizes a mix of the one-time secret key, as the first validation variable, and credentials remain on a cell phone, as the second component, to offer a reliable and secure confirmation approach. They additionally display an experimental analysis of the security and convenience of this instrument. The security convention is dissected against a foe model; this assessment demonstrates that their technique is protected against different malicious behaviors, in particular, key logging, shoulder surfing, and phishing assaults.

Rossi et al. [7] shown a review of the two component confirmation scene and address the issues of close versus open arrangements. They presented a novel public norms based confirmation innovation that they had created and discharged in open source. They then gave a characterization of two mobile confirmation changes.

The study of Ganesan et al. [8] has proposed "A Novel Digital Envelope Approach for A Secure-Commerce Channel" the first envelope in Java consolidating the best of both symmetric (AES) and asymmetric (HECC over GF(p) of Genus 2) procedures. They have tried the calculation for different sizes of documents. To guarantee respectability of the information, they have received the MD5 hash calculation. In this work, they have composed and actualized HECElG Algorithm (HEC-ElGA) for the particular era, encryption and decoding forms furthermore,

received a probabilistic optimality checking (is Probable Prime() in Java) to figure out if the given number is prime or not. To figure out if the given number is prime or not, one needs to utilize AKS calculation which is deterministic in nature.

The study of Gupta and Silakari [9] has illustrated "A test study on Performance Evaluation of Asymmetric Encryption Algorithms" of the study of Elliptic Curve Cryptosystem (ECC) utilized as a part of numerous applications. ECC is a when contrasted with RSA and discrete logarithm frameworks, is a superior alternative for what's to come. Consequently, ECC is such a brilliant decision for doing deviated cryptography inconvenient gadgets at this moment. The littler ECC keys it turns makes the cryptographic operations that should be performed by the conveying devices to be inserted into significantly small and portable equipment, such that the product application will finish cryptographic operation with reduced processor cycles, process are carried at high speed while retaining security. This implies the reduced force utilization, reduced space expended on printed circuit board, programming applications dashing make fewer memory requests. In a nutshell, for correspondence utilizing littler gadgets and asymmetric cryptosystem, they require ECC.

Jamgekar and Joshi [10] have presented "Record Encryption and Decryption Using Secure RSA" a modified RSA algorithmic evaluation to secure document transmission. RSA calculation is awry key cryptography additionally called Public Key cryptography. Two keys are created in RSA; one key is utilized for encryption &other key which is just known not beneficiary can decode the message. No other key can decrypt the message. Each imparting party needs only a key pair for speaking with any number of other conveying parties. When somebody acquires a key pair, he/she can talk to any other person. RSA is a plainly understood public key cryptography calculation and was one of the first significant advances out in the public key cryptography. Regardless of the fact that it is a dynamic calculation, it is powerless against assailants. With the assistance of all beast power assaults, a program can get the private key.

Alanazi et al. [11] have exhibited "Utilizing Public Key Cryptography as a part of Mobile Phones" of the significance of the security of the EMR and the patients' rights. Furthermore, cryptography calculations and security prerequisites have been talked about and the paper has likewise examined distinctive construction modeling, plans and frameworks that have been accounted for in the writing. More or less, a significant portion of these structures are weak as far as accomplishing the security prerequisites, while on the other side, the greater part of the frameworks have not talked about the patients' rights and how the framework can identify the persons who show these records.

Ho et al. [12] have explored "examination of secure methodologies which can apply to mobile commerce business" of the standard of solid exchange component in mobile commerce trade: “Wireless Transport Layer Security (WTLS)” and “Kerberized” or “KiloByte SSL” (KSSL). Under the examination, they find that the security level of WTLS utilized in a cell phone still lacks at present. As of late, WAP clients have considerably diminished. In this manner, KSSL being employed in WAP to recover the disadvantage of WTLS and how to guarantee the security in versatile EC are future headings.

III. Problem Description

The previous section discussed about various existing studies associated with authentication issues of m-commerce services where most of the studies focused on mitigating the security issues using some mutual authentication system in between the cloud-based client-server architectures. Security is considered as a real-time key component in M-commerce. It can be seen that the design specification associated with the security architecture in the customary frameworks of m-commerce has a propensity of trading off the client's close to personal information alongside the record certifications transmitted through a network system.

GSM gives a moderately secure association through the PIN (Individual Identification Number) at the time of turning on the handset. A verification convention in the middle of the handset and the system through SSL encryption of voice and information is likewise there in GSM. In any case, it is insufficient to persuade individuals. To get the certainty minimum amount of customers, more is normal in the field of security. It looks that the Master cards will be the favored method for accessing a protected framework. The smart card can be as a Visa or as

an SIM like a little card. It is conceivable to run an assortment of use on a solitary little SIM card. Encryption is being utilized to guarantee classification through a mystery key in the relationship with the algorithmic evaluation.

This delivers a different rendition of the first message that the beneficiary can decode utilizing the first key to recover the substance. The key must be kept mystery between the two identities. There are two main systems, which can be utilized to scramble a record: symmetric and unbalanced. With the symmetric strategy, the same key is utilized for encryption and decoding. The issue is that the key must be transmitted to the beneficiary of the message, and an outsider could access the key amid this transmission. Inside symmetric encryption, both sides have a key of 1024, 2048 bits commonly. Utilizing unbalanced calculation, otherwise called open key techniques, an arrangement of two keys is utilized a private and an open key. Data encoded utilizing the public population key must be recovered utilizing the integral private key.

The future perspective of cloud-based networks brings a key challenging scenario that organizations will confront as they assemble organizations for the remote and wired age is that they should coordinate abilities and disciplines that are very separate in many associations today. These incorporate inventive considering, prepared business abilities, a profound comprehension of innovation and particular issues in information transfers and data frameworks, a comprehension of how this will develop, and all around sharpened aptitudes in outline and marking. Going ahead from here, opens door for accomplishment in m-commerce will go to the individuals who concentrate on making convincing worth for clients. Established in a profound comprehension of the portable experience, who assemble dynamic infrastructures for the business, and who manufacture plans of action that reap reasonable quality from the offerings and financial matters associated with the mobile Web.

The next section introduces the design specifications related to the proposed system followed by the implementation and the result analysis respectively.

IV. Proposed System

The proposed system aims to develop a secure and novel android based multi-level security model for preserving the identity and the financial credentials associated with a customer during an online transaction. In m-commerce systems and applications it is very challenging to avoid the information leakage during a financial transaction. The proposed model includes three major modules which are 1. Customer Module 2. Merchant Module and 3. Banking Module respectively. The main modules are also extended with several sub modules to achieve optimal performance metric of the proposed system. The proposed model has been designed and implemented based on a cloud-based distributed multi-server architecture. The proposed framework uses an Android application for providing a user-friendly, light-weight user interface on customer's mobile devices for performing the online transaction with a high level of security for preserving identities of entities involved in the transaction process.

The design specification associated with the proposed system also ensures a financial transaction without revealing personal details of entities to each other or with the Trusted Third Party (TTP) component. The proposed system uses three different kinds of cryptography techniques such as AES, MD5 and also random key generation to provide an improved encryption facility. It also uses the device ID, which is an IMEI number and IMSI number which is SIM ID for the successful authentication process of the user along with the android device. During the transaction process only hash data is transmitted through the network where the probability of revealing the real data by the intruders is zero. The following figure shows the architecture of the proposed system.

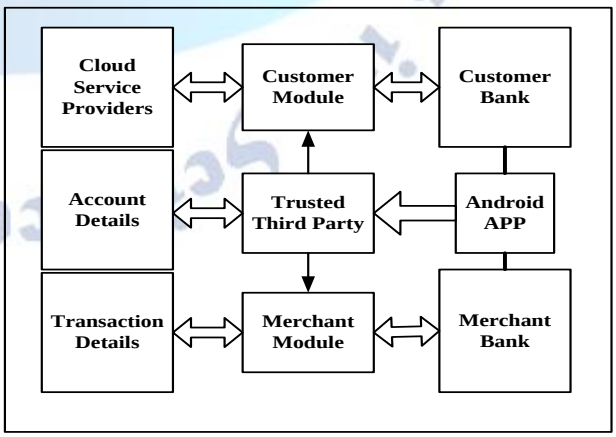

Figure-1 Schematic diagram of the proposed system

In the above-stated design of the proposed system illustrates three major modules of the project where customer module is responsible for

gathering customer details such as (Account information, transaction details, device ID and IMSI number, etc.). The banking module configures both the client bank and merchant bank with the Trusted Third Party (TTP) which is defined as an authentic way of financial transaction. To enable the m-banking services firstly a customer should provide a one-time key supplied by the bank. An auto-generated secret code will be provided to the client at the end of the successful authentication. TTP controls the transaction, and it acts as an intermediately in-between the customer bank module and the user bank module. Lastly, the Merchant module includes the details of different vendors; products, etc. and generates the invoice after a successful purchase made by any customer.

V. Implementation

The implementation of the proposed system has been carried out using Android Development Tool, where three different type of modules such as 1. Customer Module, 2. Bank Module and 3. Merchant Module has been introduced. Three stages of authentication process have been utilized to improve the data encryption process.

The Figure-2 below illustrates the database used for the developing of the application. The database contains mainly two parts as shown in figure 2. It provides the details of the banking related to the both the customer as well as the vendor with various details like their personal information, financial transaction and so on. Another part is the M-commerce part which contains the details of the different suppliers and different categories of products available and the customer's interaction with the m-commerce such as selected products and so on.

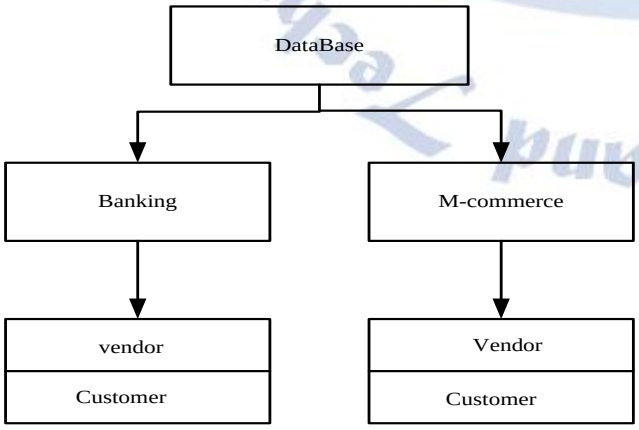

Figure-2 Classification of the Database

A. Android application for secure m-commerce.

The project uses a application developed using Android, this application allows the user interaction and performs m-commerce activity as a well secure financial transaction through m-banking. The Android application acts as the interface between the m-commerce system, m-banking, and customer. The advantage of the use is since the application resides on the user device it can be used in mobility and avoids the hassle of waiting or going to the dedicated bank or shop. The core parts of the projects are developed using Java program which provides significant features like portability, architectural neutrality and so on. The application also takes advantage of different Java technologies like JSP, which provide the server side interaction required for performing a different task such registering, login and transactions.

B. Banking secret key

The banking secret key or activation key is a crucial part of this application; here the banking is performed by both entities like customer and the vendor. The banking operation carried is through the mobile banking or m-banking. The logical operation and implementation of the banking process are illustrated in the form Pseudo code in this section. The description provides interpretation of true code implementation.

C. Pseudo code for Banking activation key or secret key.

Banking secret code pseudo code is explained below with its relevant input, variable initialization, and necessary computational functions.

Start
Input: IMEI, IMSI, CST ID
Output Secret key (sKey)
Start:

CST $\xrightarrow{\text{creates}}$ Bank account

CST $\xrightarrow{\text{provides}}$ Credentials

Bank $\xrightarrow{\text{Provides}}$ new CST a/c

CST $\xrightarrow{\text{request}}$ m-bank activation

Bank $\xrightarrow{\text{checks}}$ CST credentials (IMEI,CST ID,IMSI)

Bank $\xrightarrow{\text{generates}}$ OAK

(IMEI, CST ID, IMSI) $\xrightarrow{\text{Randomkeygenerator}}$ OAK.

END

D. Hashing Function

The hashing function is a significant process in enhancing the security of the proposed system. It is specifically used to provide robustly as well as secured financial transaction by preserving the identity of the entities involved. The hashing function is obtained using cryptography algorithm, cryptography algorithm such as SHA1 is used to enhance security. This particular hashing is performed to store the secret code of the customer by the TTP.

Input: Customer secret code (Scode)

Ouput: HScode

Start:

CST $\xrightarrow{\text{Initiates}}$ payment

TTP $\xrightarrow{\text{performs}}$ CST validation

TTP $\xrightarrow{\text{Checks}}$ CST (IMEI, CST ID)

TTP $\xrightarrow{\text{receives}}$ CST Scode

CST Scode $\xrightarrow{\text{Subjected}}$ SHA1

SHA1 (CST Scode) $\xrightarrow{\text{results}}$ HScode.

End

Where CST represents the customer, IMEI represents international mobile equipment identity number used to identify mobile device, IMSI represents the global mobile subscribers identity is unique for all sim card.

VI. Result Discussion

This section discusses about the significant findings of the proposed study. It also highlights a comparative analysis in between the SHA and other hash algorithms. The experimental prototyping the proposed system has been evaluated considering three different type of analysis one is 1. Timing analysis 2. Security Space analysis.

The Experimental prototyping shows that the application is very much feasible and robust with respect to the android platforms. Some specific entities such as light weight, Easy to use these types of features includes more efficiency and scalability of the proposed system. To evaluate the effectiveness of the proposed algorithm timing analysis is used to calculate the efficiency of the SHA 1 algorithm as compare to conventional SHA-192 algorithms. The following table shows the timing analysis associated with the secure hash algorithms.

Table-I

File Size (KB)	Processing Time (Sec)	
	SHA-1	SHA-2
5	0.109	0.639
10	0.374	1.138
15	1.435	3.151

The above table shows the effectiveness of the proposed system on two different performance parameters. File Size and Processing Time are considered as performance parameters of the proposed system. The security analysis and the prototyping show that the impact of avalanche effect is more on SHA-1 as compare to the conventional SHA-192 family.

Conclusion

The major issues associated with the m-commerce applications are to protect the user identity as well as the financial details during the process of online transactions. Mobile application systems will probably be significantly unique about the conventional client model, which makes a scope of new security exposures. It is basic to comprehend these exposures and plan systems in light of security before conveying applications and after that retro-fitting security. This paper presents a novel architecture and their natural exposures which present a scalable, secure and multi factorial hash based security model for mobile payments using android devices. The proposed work ensures secure protocols for portable/mobile applications. The proposed system uses some practical encryption algorithms such as SHA (Secure Hash Based Algorithm), IMEI and MD5.The experimental outcomes show the effectiveness of the proposed system concerning robustness, usability and computation time.

REFERENCES

[1] Wasnik, T. P., Vishal S. Patil, Sushant A. Patinge, Sachin R. Dave, and Gaurav J. Sayasikamal. "CRYPTOGRAPHY AS AN INSTRUMENT TO NETWORK SECURITY." *International Journal of Application or Innovation in Engineering & Management (IJAIEM)* 2, no. 3 (2013): 72-80.

[2] Chavan, Sachindra K., and M. L. Bangare. "Secure CRM Cloud Service using RC5 Algorithm." *International Journal of Computer Trends and Technology-volume4, Issue3-2013.*

[3] Sameer, Hasan Al-Bakri, and MahabubulAlamGazi. "Securing peer-to-peer mobile communications using public key cryptography: New security strategy." *International Journal of Physical Sciences* 6, no. 4 (2011): 930-938.

[4] Rahma, Abdul Monem S., Rabah N. Farhan,and Hussam J. Mohammad. "HYBRID MODEL FOR SECURING E-COMMERCE TRANSACTION." International Journal of Advances in Engineering & Technology 1, no. 5 (2011).

[5] Sung, S., Youn, C., Kong, E. and Ryou, J., 2015, January. User authentication using mobile phones for mobile payment. In Information Networking (ICOIN), 2015 International Conference on (pp. 51-56). IEEE.

[6] Mallat, N., Rossi, M. and Tuunainen, V.K., 2004. Mobile banking services.Communications of the ACM, 47(5), pp.42-46.

[7] Ganesan, Ramachandran, Mohan Gobi, and KanniappanVivekanandan. "A Novel Digital Envelope Approach for A Secure E-Commerce Channel." *IJ Network Security* 11, no. 3 (2010): 121-127.

[8] Gupta, Kamlesh, and Sanjay Silakari. "ECC over RSA for Asymmetric Encryption: A review." *International Journal of Computer Science Issues* 8, no. 3 (2012): 370-375.

[9] Jamgekar, Rajan S., and GeetaShantanu Joshi. "File Encryption and Decryption Using Secure RSA." *International Journal of Emerging Science and Engineering (IJESE)* 1, no. 4 (2013): 11-14.

[10] Elbaz, Limor. "Using public key cryptography in mobile phones." *Discretix Technologies Ltd. White Paper* (2002).

[11] Ho, Hann-Jang, and RongJou Yang. "A comparison of secure mechanisms for mobile commerce." In *Proceedings of the 7th WSEAS International Conference on Mathematics & Computers in Business & Economics*, pp. 24-28. World Scientific and Engineering Academy and Society (WSEAS), 2006.