Improving Banking Authentication Using Hybrid Cryptographic Technique

Arpit Agrawal
Asst. Professor, Dept. Of Computer Engineering
Institute Of Engineering & Technology
Devi Ahilya University, Indore, India

Sant Choubey
Dept. Of Computer Engineering
Institute Of Engineering & Technology
Devi Ahilya University, Indore, India

***Abstract*-- The online banking environment has grown tremendously over the past several years and will continue to grow as financial institutions continue to strive to allow customers to complete money transfers, pay bills, and access critical information online. During this same time, online banking has been plagued by Internet criminals and fraudsters attempting to steal customer information. Phishing, pharming, and other types of attacks have become well known and are widely used as a means for fraudsters to obtain information from customers and access online banking accounts. As a result, authenticating customers logging onto their online banking service has become a crucial concern of financial institutions. This research study portrays a clear picture of the need for enhanced authentication in online banking. It presents the main security concerns and criminal activities that are driving the need for stronger authentication, as well as showing the growth of the online channel that is being driven by consumers and financial institutions. This study simplifies and provides a resource for understanding the many options available when implementing enhanced authentication in the online banking environment. It provides detailed analysis of the many authentication solutions available, as well as a set of guidelines for selecting and implementing enhanced authentication, based on the learning and knowledge of industry experts and the consumer.**

***Index Terms*— Authentication, Encryption, Hybrid cryptography, Multi factor authentication, Online banking security.**

I. INTRODUCTION

Online banking systems have become quite popular in the last ten year. Customer from an online bank can manage their accounts with electronic device like smart phone, tablet and personal computers. Ultimately the customer is owner of these account that's why whatever they want to do like transaction of money from one account to another account and pay bill etc.do in easy way. This things also overcome the load of bank clerk and the online banking is 24x7-hour open so customer better use this facilities. Security of online banking is very challenging issue as concern of banking service provider bank and as well as customer. Otherwise in minute customer losses money and bank losses there trust. There are some protocol required for communication between client and server. This protocol is called TCP/IP. TCP/IP protocol use for standard communication between client and server but when we taking about secure data transmission than TCP / IP protocol is insecure because data packets flowing through TCP / IP networks are not normally encrypted. Thus, anyone who interrupts communication between two machines will have a clear view of the data, passwords. This has been addressed through Secured Socket Layer (SSL), a Transport Layer Security (TLS) system which involves an encrypted session between the client browser and the web server. One of the biggest attractions of Internet as an electronic medium is its openness and freedom. It is a public domain and there is no restriction on who can use it as long as one adheres to its technical parameters. This has also given rise to concerns over the security of data and information transfer and privacy. It will be sufficient to say here that the key components of such concern are, authentication, authorization, confidentiality of data, data integrity and non-repudiation.

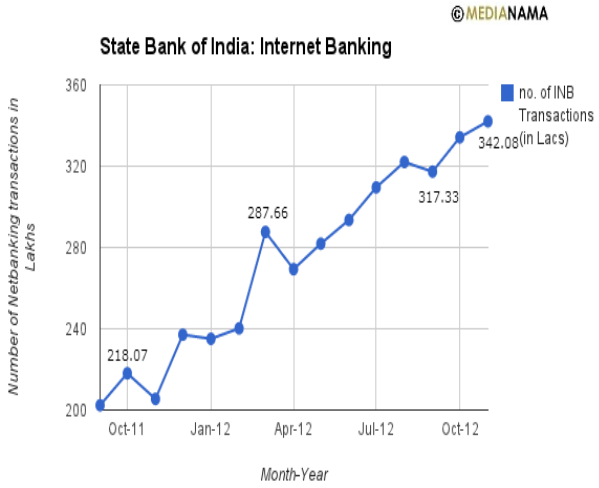

Fig 1.SBI Net Banking Transaction Report.

In this graph we can see that popularity of online banking is increased in recent year. This report is only one year of SBI bank [11]. There are many banks provide online banking in market.

ISSN: 2278 – 1323

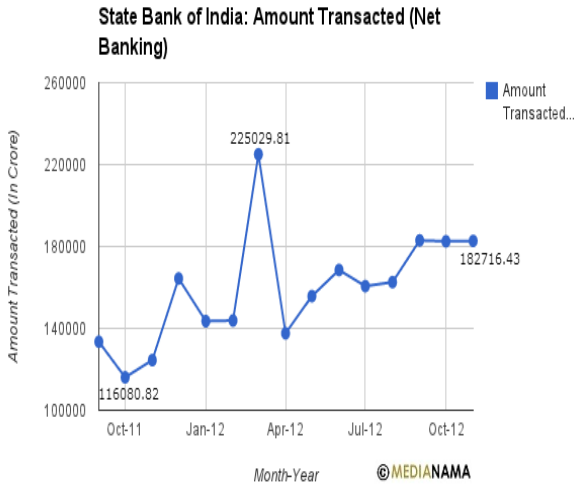

Fig 2.amount transacted using net banking in SBI.

As we see in above report [11] that there are millions of money transected through online banking. This report only in SBI but many banks in India provides online banking so u can imagine that a lot of money transfer or use online, this situation open hackers eye to grab your money using online fraud. That's why security is must important in online banking.

1.1 SECURITY ISSUES IN ONLINE APPLICATION (E-BANKING)

Internet is a public network of computers which facilitates flow of data / information and to which there is unrestricted access. Banks using this medium for financial transactions must have proper technology and systems in place to build a secured environment for such transactions. Security risk arises on account of unauthorized access to a bank's critical information stores like accounting system, risk management system, portfolio management system, This may result in loss of data, theft of or tampering with customer information, disabling of a significant portion of bank's internal computer system thus denying service. There are two key issue in online banking first is how to authenticate genuine person who use banking services and the second key issue is how to transfer sensitive data over network in secure manner. Here we discuss some issues in online banking system.

1.1.1 Authentication

The term authentication describes the process of verifying t he identity of a person or entity. It is the process of determin ing whether someone or something is, in fact, who or whatit is declared to be. Authentication is part of most online applic ations.Before a user can access its email account, its online b anking account or its favorite online shopping account.it has to identify and authenticate itself to the application. The most common form of authentication is done through th e use of passwords.

1.1.2 Authorization

While authentication verifies the user's identity, authorization verifies that the user in question has the correct permissions and rights to access the requested resource. As you can see, the two work together. Authentication occurs first, then authorization.

1.1.3 Data Confidentiality

The concept of providing for protection of data from unauthorized disclosure is called data confidentiality. The biggest concern will be to keep information private that's why we have to develop secure cryptographic system. Whether it is password send during a log on process.

1.1.4 Non-Repudiation

Non-Repudiation involves creating proof of the origin or delivery of data to protect the sender against false denial by the recipient that data e.g. a customer may request a transfer of money from his account to be paid to another account, later, he claims never to have made the request and demands the money be refunded to the account. if we have non-repudiation through cryptography, we can prove usually through digitally signing the transaction request, that the user authorized the transaction.

1.1.5 Integrity

When the content of message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost. We can use cryptography to provide data is not viewed or altered during storage or transmission.

1.2 USER AND BANK RELATIONSHIP

Bank is service provider in different manner like customer can open account; save money in account and bank give some interest to customer. Now days bank give many online services like make online transaction, balance enquiry, pay e-bill, request to cheque book, add beneficiary ,transfer money one to another account etc.

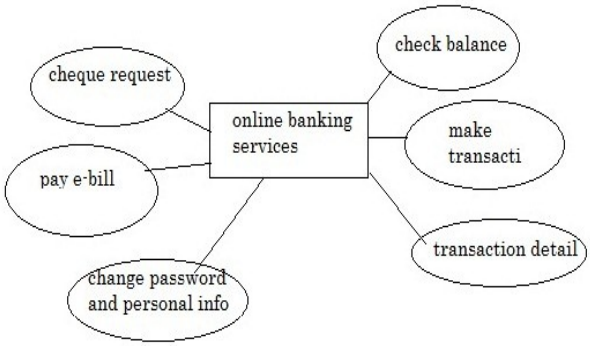

Fig 3. Online banking services to users

Costs of banking service through the Internet form a fraction of costs through conventional methods. Rough estimates

assume teller cost at Re.1 per transaction, ATM transaction cost at 45 paisa, phone banking at 35 paisa, debit cards at 20 paisa and Internet banking at 10 paisa per transaction [12]. The cost-conscious banks in the country have therefore actively considered use of the internet as a channel for providing services.

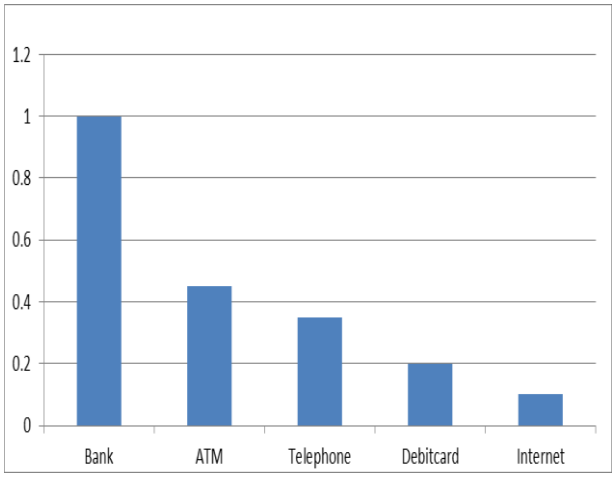

Fig 4 cost of per transaction using different banking services

1.3 LOOP AND HOLES IN CURRENT BANKING SYSTEM

Modern security techniques have made cracking very difficult but not impossible. Furthermore, if the system is not configured properly or the updated patches are not installed then hackers may crack the system using security hole. A wide range of information regarding security hole and their fixes is freely available on the Internet. System administrator should keep himself updated with this information. When a banking system is connected to the Internet, an attack could originate at anytime from anywhere. An attack could be any form like. The intruder may gain unauthorized access and destroys, corrupt or alters data and denying access to privileged users. There are common attacks in online banking system given below.

1.3.1 Keystroke Capturing/Logging

Anything you type on a computer can be captured and stored. This can be done using a hardware device attached to your computer or by software running almost invisibly on the machine. Keystroke logging is often used by fraudsters to capture personal details including passwords. Some recent viruses are even capable of installing such software without the user's knowledge. The risk of encountering keystroke logging is greater on computers shared by a number of users, such as those in internet cafes. An up-to-date antivirus software program and firewall will help remove the harmful software before it can be used. In now days many banks are using virtual keyboard for taking users input. Virtual keyboard prevents from this type of attacks.

1.3.2 Pharming

Pharming is when a fraudster creates false websites in the hope that people will visit them by mistake. People can sometimes do this by mistyping a website address – or sometimes a fraudster can redirect traffic from a genuine website to their own. The 'pharmer' will then try to obtain your personal details when you enter them into the false website.

1.3.3 Phishing

Phishing involves an e-mail message being sent out to as many internet e-mail addresses as the fraudster can obtain. Usually, these e-mails claim to come from a legitimate organization such as a bank or online retailer. The e-mail requests the recipient to update or to verify their personal and financial information, including date of birth, login information, account details, credit card numbers, PINs etc. The e-mail will contain a link that takes you to a spoof website that looks identical (or very similar) to the organization's genuine site. The fraudster can then capture personal data such as passwords. Clicking on a link may also download malware onto your computer, which will record your future use of the internet and forward even more information to the fraudster. The fraudsters will then use this information to compromise bank accounts, credit cards etc.

1.3.4 Identity Theft

Identity theft is a crime in which a fraudster obtains key pieces of personal information, such as date of birth, bank details or driver's license numbers, in order to impersonate someone else. The personal information discovered is then used illegally to apply for credit, purchase goods and services, or gain access to bank accounts

.

1.3.5 BruttforceAttack

It is an automated process of trial and error used to guess a person's user name, password, credit card number or cryptographic key. A normal brute force attack uses a single user name against many passwords. A reverse brute force attack uses many user names against one password. When a guessed password allows access to the system, the brute force attack has been successful and the attacker is able to access the account. Brute Force techniques are highly popular and often successful in systems with millions of user accounts.

1.3.6 Denial-Of-Service (Dos) Attacks

DoS attacks can temporarily incapacitate the entire network or at least those hosts that rely on TCP/IP. DoS attacks strike at the heart of IP implementations. Hence they can crop up at any platform; a single DoS attack may well work on several

ISSN: 2278 – 1323

target operating systems. Many DoS attacks are well known and well documented.

1.3.7*SnifferAttack*

Sniffers are devices that capture network packets. They are a combination of hardware and software. Sniffers work by placing the network interface into promiscuous mode. Under normal circumstances, all machines on the network can "hear" the traffic passing through, but will only respond to data addressed specifically to it.

1.3.8Holes

A hole is any defect in hardware, software or policy that allows attackers to gain unauthorized access to your system. The network tools that can have holes are Routers, Client and Server software, Operating Systems and Firewalls. That causes the network to fail, reboot, and hang.

2 BACKGROUND

2.1 PASSWORD MANAGEMENT AND AUTHENTICATION MANAGEMENT

Authentication is simply the process of proving that a person is who they say they are. A user must perform authentication to prove their identity to a bank before a session is initiated in which bank accounts can be managed. This is referred to as entity authentication. Furthermore, it is possible that an extra authentication step is required to authorize the transfer of money this is called transaction authentication. There are some factors in authentication which is used:

A. Knowledge:

Something you know. This covers things like passwords, Father's maiden name, the name of one's pets, and so on. Banks commonly use these when you call them over the phone and need to prove you are who you say you are.

B. Possession:

Something you have. Things like keys, access cards, etc.

C. Existence:

Something you are. The shape of your face, the tone of your voice, your fingerprints, and the geometry of you hand. These are called biometric authenticators.

As mentioned earlier, authentication is a process to verify the claimed identity. There are various techniques available for authentication. Password is the most extensively used method. Most of the financial institutions use passwords along with PIN (Personal Identification Number) for authentication. Technologies such as tokens, smart cards and biometrics can be used to strengthen the security structure by requiring the user to possess something physical. There are three commonly classified levels of verification.

Level-1:
The first and most common are a simple ID and password.

Level-2:
The second level requires additional verification, such as a personal item (mobile phone, token, security card and etc.).

Level-2:
The final level demands the use of the user's biological information, such as a finger print, face recognition and etc.

Two factor authentication systems combine two of the three levels of verification. Three factor authentications required all of three levels. One typical example of two factor authentication is a combination of the first level, ID and password, and the second, an OTP (One Time Password). Currently, smart phones are the most common source of the OTP. Generally most of bank use two factor authentication at least e.g. PNB bank uses two password one for login other for transaction, SBI bank uses one for login and second as OTP for transaction etc. as we see the popularity of online banking, bank have to ensure that the user identity ,personal information and money will be secure. All online service provided by bank should must be secured. Bank use some basic security features to identify genuine user by using authentication techniques and data transfer to user end to server end by using different cryptographic techniques. For authentication generally we check user id and password which is breakable by using bruttforce attack for this reason bank uses another level of authentication like OTP, OTP is send to registered mobile device but there is another aspect of security like picture authentication. in our purposed authentication technique we use all the technique like password, question answering and picture with tag and OTP [2]. For data transfer we have to hide our data to the external user or in network. The process of disguising a message in such a way as to hide its substance is called encryption. An encrypted message is called cipher text. The process of turning a cipher text back into plain text is called decryption. Cryptography is the art and science of keeping messages secure. It uses a 'key' for encrypting or decrypting a message. Both the method of encryption and the size of key are important to ensure confidentiality of a message.

There are two types of encryption: Symmetric key and Asymmetric key encryption. In the symmetric key cryptography scheme, the same key is used to encrypt and decrypt the message. Common symmetric algorithms include One-time pad encryption, Data Encryption Standard

(DES), Triple DES, LOKI, Blowfish, and International Data Encryption Algorithm (IDEA). DES and Triple DES are the commonly used techniques. Asymmetric key cryptography scheme is also known as Public key crypto-system. Here two keys are used. One key is kept secret and therefore it is referred as "private key". The other key is made widely available to anyone who wants it, and is referred as "Public key". The Public key and Private Key are mathematically related so that information encrypted using the public key can only be decrypted by the corresponding private key and vice-versa. Importantly, it is near to impossible to find out the private key from the public key. Common and more popular public key cryptosystem algorithms are Diffie-Hellman, RSA, Elliptic Curve etc. In all these, the confidentiality is directly related to the key size. Larger the key size, the longer it takes to break the encrypted message. Diffie-Hellman: This is the first public key algorithm invented. It gets its security from the difficulty of calculating discrete logarithms in a finite field. Diffie-Hellman method can be used for distribution of keys to be used for symmetric encryption. That's why we use combined algorithm elliptic curve diffie-hellman cryptography (ECDH) for encrypt data which travels in network.

3 REVIEWS

In most cases of authentication technique and trend is user id and password which is use for first level of authentication and second level of authentication uses as OTP. But for receiving OTP you have Mobile device .some new trend comes in now days QR code authentication which is new technique [1] but in this technique we have also required smartphone which is not possible to have everyone which uses banking services. For authentication we use some cryptographic algorithms like MD5 for Hash generation [2] but in recent year Md5 found vulnerable that's why we using SHA-1 algorithm for hah generation which is also RBI (Reserve Bank Of India) standards. For preventing bruttforce attack we use picture with tag based authentication which is not breakable [4]. MD5 hash algorithm is breakable and it is possible to collision attack [10]. When we taking about hash generating algorithm than simple hash algorithm with key length 128 bit is secure [9] and as well as SHA-1 haven't found collision attack[8].

4 PROPOSED WORK

A number of applications are developed now in these days for providing support to their customers for 24X7 manners. Some of these applications are frequently used in our daily life such as online banking, email accounts and others. These applications need strong authentication management system by which the only system owner can get their sensitive and private data. In this presented work banking system and their security issues are targeted to improve in terms of authentication and data security management. On the other hand the security in the current banking system having some lakes which is desired to improve listed below:

A. Less Secure Authentication Technique:

The authentication system consumes weak attributes for performing end client authentication, therefore security during authentication management is poor, thus desired to improve the authentication technique.

B. Computationally Expensive Cryptographic Approach:

The implemented cryptographic techniques are computationally fragile and consume higher space and time for encrypting fewer amounts of data. Thus desired to improve the efficiency of cryptographic techniques.

Therefore a new kind of security integration is desired which improve the computational cost and delay in network during the authentication process by efficiently applying the security techniques and improving the security in layered architectures. Online banking is now in these days an essential application for business and personal purpose. These applications are provides end to end customer support for making payments performing fund transfer and other financial support. The proposed work provides the solution for online banking security and authentication management. By which the bank frauds, phishing and man in middle kind of attacks are prevented. In addition of that by mutual communication the authentication management is obtained.

The proposed banking application is developed to simulate the authentication management and for simulation of secure transactions between user and banking application server. Therefore the presented prototyping model is desired to simulate using the a web based application which includes all the security features by which only authorized user can gain access to the system.

5 PROPOSED METHODOLOGY

In order to provide end to end security in the proposed banking application the following functions are desired to implement.

ISSN: 2278 – 1323

A. Implementation of Authentication System:

The proposed authentication system is a five phase authentication system, which involve the following steps of authentication.

a. User Id
b. User Password
c. Security Question Answering
d. Picture Authentication
e. One Time Password

B. Implementation of Lightweight Cryptographic Algorithm for Efficient Encryption and Decryption:

In order to develop the lightweight hybrid cryptographic technique the following algorithms are hybridized.

a. Elliptic Curve Diffie Hellman (ECDH) Algorithm-

ECDH is an Elliptic Curve variant of the standard Diffie Hellman algorithm. ECDH is used for the purposes of key agreement. It requires less computational power, communication bandwidth, and memory when compared to other cryptosystems. Elliptic Curve Cryptography (ECC) & Diffie Hellman algorithm combined is a newer alternative to public key cryptography. ECC operates on elliptic curves over finite fields. The main advantage of elliptic curves is their efficiency. They can offer the same level of security for modular arithmetic operations over much smaller prime fields. Thus, the relative performance of ECC algorithms is significantly better than traditional public key cryptography. There are two variant of ECC first is ECDH and second is ECDSA. ECDH is a method for key exchange, and ECDSA is used for digital signatures. In our proposed system we use first variant ECDH.

b. Simple Hash Algorithms (SHA-1) –

A hash function is simply an algorithm that takes a string of any length and reduces it to a unique fixed length string. Hashes are used to ensure data and message integrity, password validity. Each hash is unique but always repeatable. That means that the word 'cat' will hash to something that *no* other word hashes too, but it will *always* hash to the same thing. The function is 'one way'. Meaning that if you are given the value of what 'cat' hashes too but you didn't know what made it, you would never be able to find out that 'cat' was the original word. There are many different hash functions but the one I will be concentrating on here is called the Secure Hash Algorithm 1 or SHA-1. SHA-1 is also called digital fingerprinting algorithms. They are irreversible functions that provide a fixed-size hash based on various inputs. These Hash algorithms provide a constant-sized output for any input, and their most important property is irreversibility. Irreversibility and collision resistance are necessary attributes for successful hash functions. SHA1 outputs a 160-bit digest of any sized file or input. Examples of hash functions are Message Digest-5 (MD5) Secure Hash Algorithm-1 (SHA-1) and SHA-256. Message Digest-5 (MD5) is a hash function that is insecure and should be avoided. SHA-1 is a legacy algorithm and thus is adequately secure.

5.1 SYSTEM ARCHITECTURE

The proposed working model and their involved processes are given in the below figure 5.

In below figure 5 a number of sequential processes are taken place. First user provides their ***User ID*** for initializing the authentication process if user is not registered then system redirect to the user for ***registration process***. If customer id found in database of bank than user go to next step for password. Than check password and if password wrong than go to previous step otherwise go to next step which is system generate random question which is submitted previously during registration process. The ***randomly generated question*** can be a date of birth, PAN card detail or any user sensitive information. If user answer all the questions than the system ask for image authentication during this process images with tags are appeared and required to select correct image and tag for successful authentication. As the user select the correct image and tag than one time password is sent to the user mobile and this one time password is used as private key for encryption. In addition of that user provides the password which is first produced into the SHA-1 algorithm for hash key generation. This hash key is used as public key for encryption algorithm. Then the generated public key and private key with the password as data is transmitted to the XOR operation after that encrypted data go to server for verification.

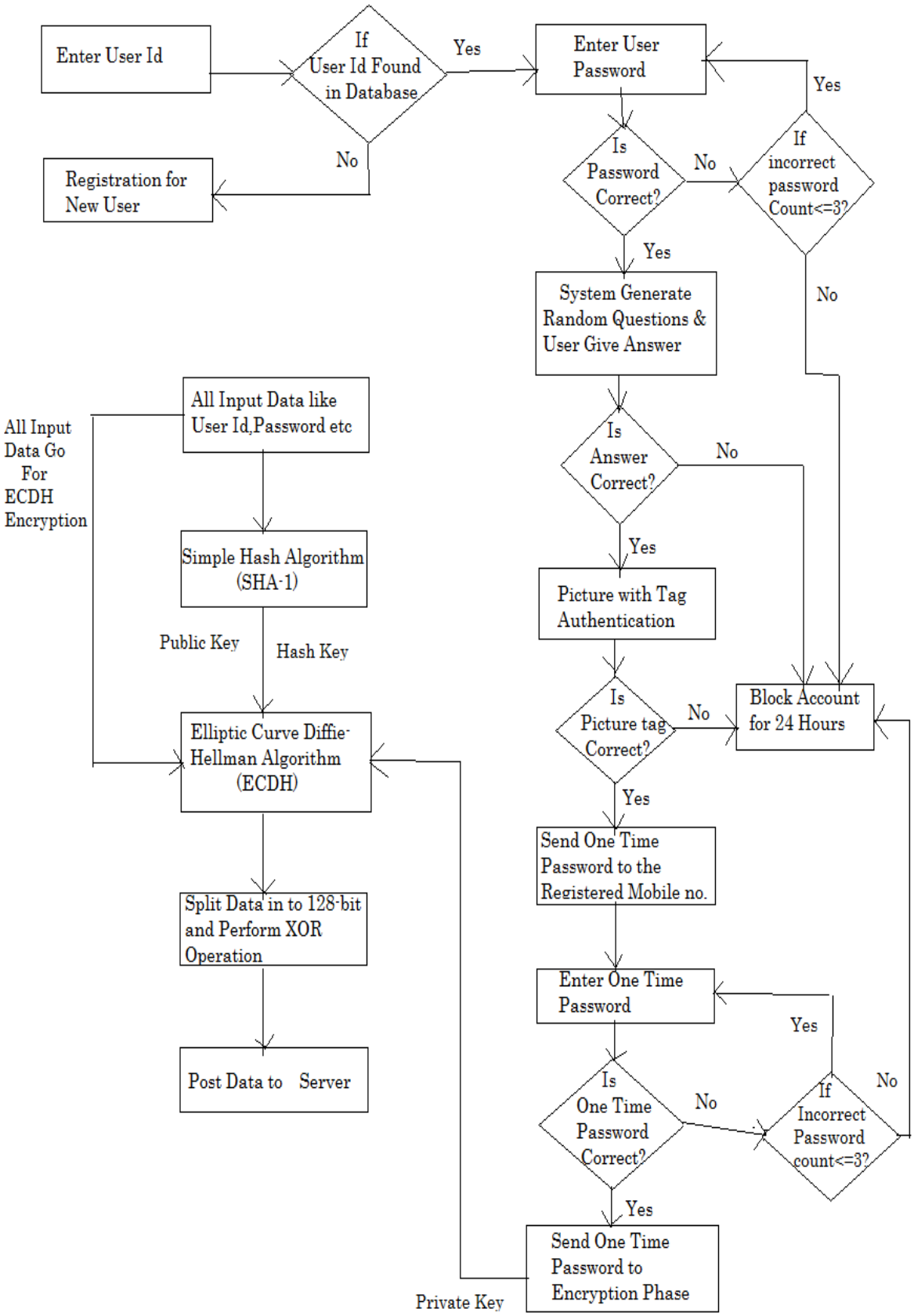

Fig 5 System Architecture

ISSN: 2278 – 1323

5.2 FLOW OF SYSTEM

Here you can see below in figure 6 flow of proposed system. There are nine subsystems which perform some small task to run our system. We will discuss to all subsystem in next paragraph.

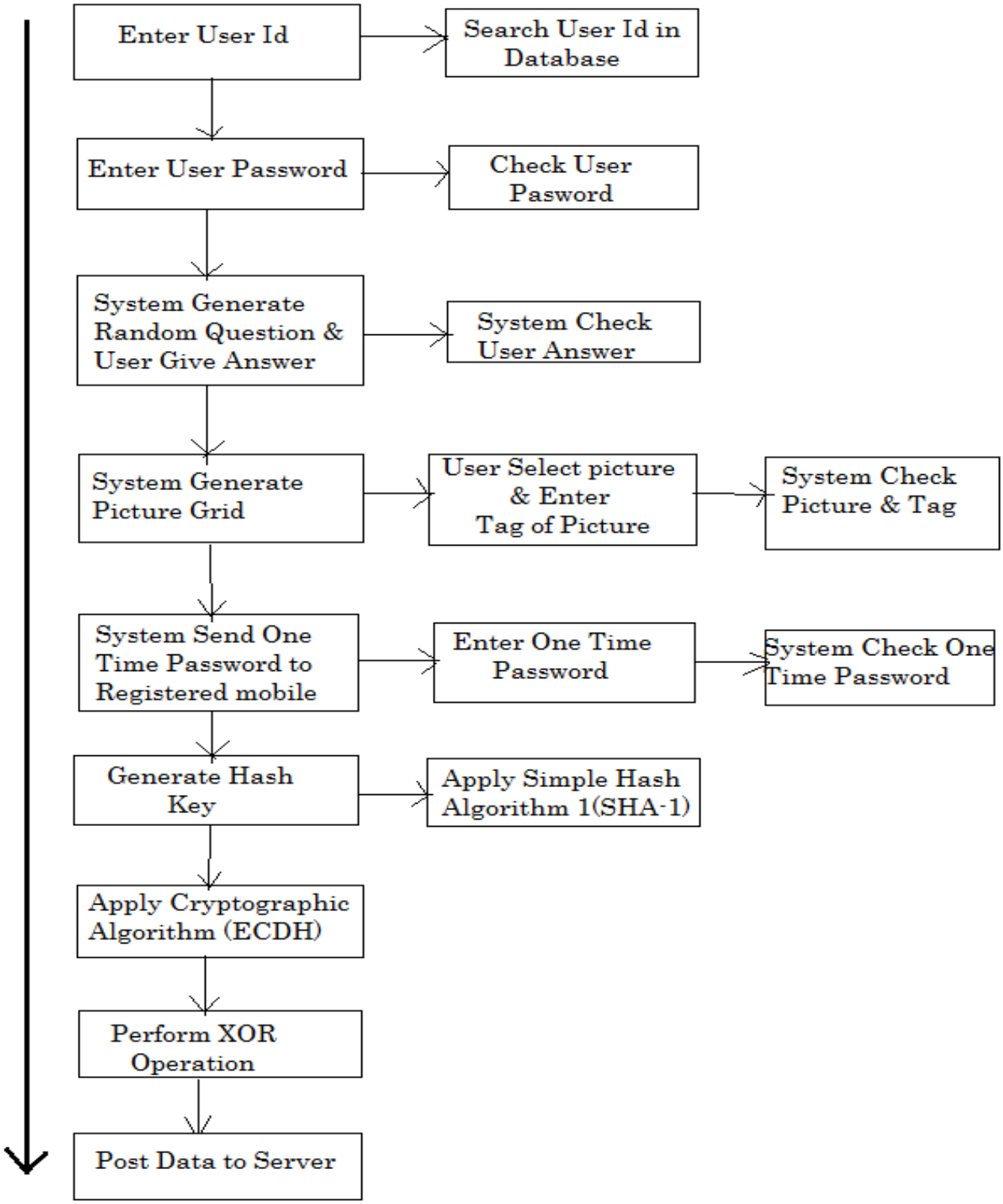

Fig 6 Flow of System

1. Taking user input as user id and whether this id is exists in database or not? These tasks perform by in this section of system.

2. User password should be alphanumeric and block account for 24 hour when user enters three consecutive wrong passwords.

3. This phase is responsible for what will be security question for user and there answer is verified by this subsystem.

4. In this phase system show picture grid and user select one picture and enter picture tag. Selected picture and tag are right or wrong check in this phase.

5. This phase send the OTP to registered mobile no and also check this OTP when user enter OTP.

6. This phase generate Hash key according to SHA-1 algorithm.

7. All input data encrypted by using ECDH algorithm in this phase.

8. In this phase split all data in 128 bit and perform XOR operation.

9. At the end all encrypted data send to the server.

6 CONCLUSION

Improving a security is not something that only has to be done once. A continuing process is required that monitors and categorized threats and opportunity. However, multi-factor authentication is not enough. Current implementations of authentication and cryptographic techniques conform user identity and secure data transmission over the network using hybrid cryptographic algorithm. In our proposed system we use multi factor like user id, password ,question answering, picture with tag and OTP so this make vary strong authentication technique for online banking security and it is not possible to easily break this techniques.

REFERENCES

[1] International Journal of Security and Its Applications Vol. 7, No. 3, May, 2013 An Innovative Two Factor Authentication Method: The QR Login System Soonduck Yoo*, Seung-jung Shin and Dae-hyun Ryu.

[2] Universal Journal of Computer Science and Engineering Technology , 133-140, Nov. 2010. © 2010 UniCSE, ISSN: 2219-2158 Eliminating Vulnerable Attacks Using One-Time Password and PassText –Analytical Study of Blended Schema M. Viju Prakash, P. Alwin Infan and S. Jeya Shobana

[3] Secure Login by Using One-time Password Authentication Based on MD5 Hash Encrypted SMS Eko Sediyono Satya Wacana Christian University Jl. Diponegoro 52-60 Salatiga, Indonesia Kartika Imam Santoso STMIK Bina Patria Magelang Jl. R. Saleh no. 2 Magelang, Indonesia Suhartono

[4] Intrusion Prevention by Image Based Authentication Techniques M SREELATHA, M SHASHI , M ROOP TEJA, M RAJASHEKAR1 and K SASANK1 IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011 MIT, Anna University, Chennai. June 3-5, 2011

[5] A Model for Securing E-Banking Authentication Process: Antiphishing Approach 2008 IEEE Congress on Services 2008 - Part I Antonio San Martino, Xavier Perramon Universitat Pompeu Fabra asm@dp-securiy.com, xavier.perramon@upf.edu

[6] Volume 4, Issue 5, May 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Infrastructure and Security Concerns on Internet Banking in India Mrs T.K. George , Dr Paulose Jacob

[7] ISSN: 2277-3754 ISO 9001:2008 Certified International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013 Review: Location Based Authentication to Mitigate Intruder Attack Dr. A.L.N Rao,Silky Puri, Shalini Rana

[8] Current Status of SHA Prof. dr. ir. Vincent Rijme DI Florian Mendel DI Norbert Pramstaller DI Christian Rechberger February 21, 2007

[9] Elaine Barker and Allen Roginsky. Transitions: Recommendation for transitioning the use of cryptographic algorithms and key lengths. NIST Special Publication, 800:131A, 2011.

[10] CERT. CERT Vulnerability Notes Database - MD5 vulnerable to collision attacks (last retrieved: 2013-10-14), December 2008. URL http://www.kb.cert.org/vuls/id/836068.

[11]Source: http://www.medianama.com/2013/03/223-chart-net-banking-transactions-by-sbi-bank-customers-from-sep-2011-to-nov-2012/

[12] Source : India Research May 29 , 2000 , Kotak Securities

ISSN: 2278 – 1323