RESEARCH ARTICLE OPEN ACCESS

E-Commerce Privacy and Security System

Kuldeep Kaur[1], Dr. Ashutosh Pathak[2], Parminder Kaur[3], Karamjeet Kaur[4]

[1]M.phil in Computer Application (Research Scholar), University College of Computer Application, Guru Kashi University, Talwandi Sabo, Punjab India

[2]Assitant Professor, University College of Computer Application, Guru Kashi University, Talwandi Sabo, Punjab, India

[3]Assitant Professor of Computer Sci, S.S Group of Colleges, Bhikhi (Mansa), Punjab, India

[4]Assitant Professor of Computer Sci, Mata Sahib Kaur Girls College, Talwandi Sabo (Bathinda), Punjab, India

ABSTRACT

The Internet is a public networks consisting of thousand of private computer network connected together. Private computer network system is exposed to potential threats from anywhere on the public network. In physical world, crimes often leave evidence finger prints, footprints, witnesses, video on security comes and so on. Online a cyber –crimes, also leaves physical, electronic evidence, but unless good security measures are taken, it may be difficult to trace the source of cyber crime. In certain e-commerce-related areas, such as networking, data transfer and data storage, researchers applied scanning and testing methods, modeling analysis to detect potential risks .In the Security system ,Questions are related to online security in which given options are Satisfied, Unsatisfied ,Neutral, Yes, No. and weak password , Strong password. it is revealed that it is quite difficult, if not impossible, to suggest that which online security is best. Online security provide the flexibility, efficiency of work, provide the better security of net banking . The main feature of the research that the data is safe in banking management for long time and open any account after along time. The Future scope of the study of Security is use to reduce threats. Security is used in the long run results in the reduction of number of branches, saying rentals of related and properties. If the better Security operate than net banking and e-marketing will be increase.

Keywords– Cryptography, Public Key, SSL, SET, Secret Key,

I. INTRODUCTION

1.1E - Commerce Privacy and Security

The most popular definition of E-Commerce is based on the online perspective of the conducted security. The Internet is a public networks consisting of thousand of private computer network connected together. A private computer network system is exposed to potential threats from anywhere on the public network .Protection against these threats requires business to have stringent security measures in place. In physical world, crimes often leave evidence finger prints, footprints, witnesses, video on security comes and so on. Online a cyber – crimes, also leaves physical, electronic evidence, but unless good security measures are taken, it may be difficult to trace the source of a cyber-crime. Security measures in e-commerce have various methods and strategies for different purposes. Different methods are suitable for specific situations, but there is no overall suitable method to foil all internet frauds for every situation. We define the possibility of a fraud as a risk. In certain e-commerce-related areas, such as networking, data transfer and data storage, researchers applied scanning and testing methods, modeling analysis to detect potential risks. . The current internet security polices and technologies fail to meet the needs of

end users. Security is the challenge and the main problem for successful e-commerce implementation as stated by many researchers.(Manjot Kaur 2012)[1]

With the fast growth of the Internet and the World Wide Web, computer and information systems have increasingly become the targets of criminal attacks and intrusions. Attacks spread very quickly and they can come from anywhere on the global. Security is a constant challenge for the acceptance and adoption of e-commerce. This was confirmed by the Kikscore survey that was conducted through the USA in August 2011. Security that governs a network is called network security .when we hear the term security, we probably think of two basic ideas:

*Protection

*peace of mind

Network security is the sum of all measure taken to prevent loss any kind. Securing our network requires co-ordination of a wide variety of security measures from creating user accounts to hiring loyal employees and keeping the server locked in a room. The current internet security polices and technologies fail to meet the needs of end users. The success or failure of an E-commerce operations hinges on myriad factors, including but not limited to the business model, the team, the customers, the investors, the product, and the security of data transmissions and storage.

Security can include encryption / decryption of data digital signature, secure socket layer, Biometric measures and firewall. Encryption plays a great role to achieve security as it is one most important techniques that is used to defend information as it travels. It is the process of converting original message that is known as plain

1.2 Security Challenges

- Internet was never designed with security in mind.
- Many companies fail to take adequate measures to protect their internal systems from attacks.
- Security precautions are expensive {firewalls, secure web servers, encryption mechanisms}.
- Security is difficult to achieve.

Public Key Infrastructure (PKI) refers to the notion that the best way to establish a system of secure communications over networks is to establish an infrastructure that will support public key encryption. The PKI would create an environment where any Internet user could "carry" certificates around that identify them in a variety of ways. Authentication of parties could become very cheap and easy. Some e-commerce proponents suggest that creation of a seamless and robust PKI would have enormous implications for speeding the growth of ecommerce.(B.J.Corbitt 2003)[2]

In general, security concerns in electronic commerce can be divided into concerns about user authorization, and concerns about data and transactions security. Data and transaction security schemes such as a secret key encryption and public/private key encryption are used to ensure the privacy, integrity and confidentiality of business transactions and message and are the basis for several online payment systems such as electronic cash and electronic checks. An attack, or intrusion, on a system is a security policy breach. Most attacks cause security policy breaches in very specific way. For example, certain attacks may enable an attacker to read specific files, but they do not allow the attacker to modify any system components. Another attack may cause a system service disruption to authorized users, but it does not allow the attacker to access any files. Although computer and network attacks vary in types and capabilities, they usually cause breaches of four different security properties of the system.

1.3 Security Aspects:-

1.3.1 Confidentiality: An attack causes a confidentiality breach if it allows unauthorized access to data.

1.3.2 Integrity: An attack causes an integrity breach if it allows unauthorized modification to the system state or data.

1.3.3 Availability: An attack causes an availability breach if it keeps authorized users from accessing a particular system resource when they need it.

1.3.4 Control: An attack grants an attacker privilege to interfere with system operation in violation of the access control policy of the system. This can lead to subsequent confidentiality integrity, availability breach.(A.Aladwani 2003)[3]

Network security and data / transaction security must be addressed simultaneously. In e-commerce security has become a high–profile concern because of the increasing number of merchants trying to spur commerce online. Unsure of security, Consumers are unwilling to provide credit card payment information over the internet. To ensure security on internet, several methods have been developed. They include: Firewalls for perimeter security, Authentication of user and servers, Encryption, and data integrity.

Security is the challenge and the main problem for successful e-commerce implementation, as stated by many researchers. However, there is wide agreement between academic researchers that security is not only a technical challenge; rather it involves managerial, organizational and human dimensions to be more effective(A. Sharma and Yurcik)[4].

Security is the basic need to secure information on internet. So confidentiality is required during transmission and it must be kept secure against all type of threats. E-commerce has become a dynamic force, changing all kinds of business operations world-wide. E-commerce is conducted on global network i.e. Internet which is untrusted. (Monjot Kaur2012, B.J.Corbitt 2003)[1, 2]

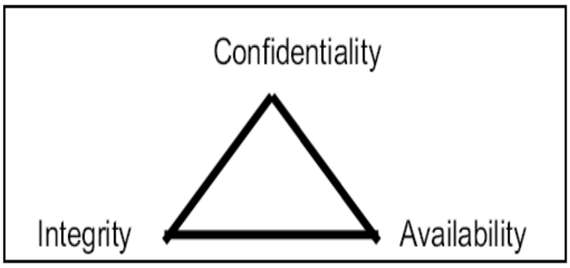
So confidentiality is required during transmission and it must be kept secure against all type of threats. The related concepts and business practices not only influence communications, the routines of daily life and personal relationships, they represent opportunities for initiating new international and domestic business ventures. Security has emerged as an increasingly important issue in the development of an e-commerce organization. (Manjot Kaur 2012)[1]

A good encryption / decryption technique guarantees to some extent that a potential intruder cannot understand the contents of the message. PGP has been considered to provide security to e-commerce. But PGP is not a full proof solution because PGP is specifically used for E-mail security which can provide Authentication and

Confidentiality, which are enough for E-mail security but not for E-commerce security. PGP cannot deal with reply and Man in the Middle security threats against E-commerce transaction.

The successful functioning of E-commerce security depends on a complex interrelationship between several applications development platforms, database management systems, systems software and network infrastructure. By doing online business, it is a facility of reaching to everyone. Exploring the opportunities challenges conventional notions of business competition through electronic flows of information and money. Payment on Internet or network is a critical important chain of whole e-commerce, which contains the payment activity. Security protection starts with the preservation of the confidentiality, integrity and availability of data and computer resources. These three tenets of information security are sometimes represented in the Confidentiality, Integrity and Authentication.(Kim C,2010)[5]

FIGURE 1.3 -The Confidentiality, Integrity and Authentication Triad



1.4 Six Security Needs in E-commerce are:
-Access Control
-Privacy/Confidentiality
- Authentication
- Non Repudiation
- Integrity
- Availability

1.4.1 Access control ensures only those that legitimately require access to resources are given access.

1.4.2 Confidentiality is concerned with warranting that data is only revealed to parties who have legitimate need, while privacy ensures that customers' personal data collected from their electronic transactions are protected from indecent and/or unauthorized disclosure. Issues related to privacy can be considered as a subset of issues related to access control.

1.4.3 Authentication provides for a sender and a receiver of information to validate each other as the appropriate entity. This means having the capability to determine who sent the message and from where and which machine.

1.4.4 Non-repudiation is a property of the transaction that positively confirms that a particular client did indeed request the transaction in question without having the ability to deny making the request.

1.4.5 Integrity ensures that if the context of a message is altered, the receiver can detect it. It is possible that as a file, electronic mail, or data is transmitted from one location to another, its integrity may be compromised.

1.4.6 Availability as defined in an information security context ensures that access data or computing resources needed by the appropriate personnel are both reliable and available in a timely manner.(P.T.Joseph 2008)[6]

1.5 Privacy

Privacy is an interdisciplinary issue. The right of humans for keeping their privacy is debated in many fields, including the areas of law, politics, philosophy, sociology, and more recently computer sciences. This may either be necessary for the e-business transaction itself (for example: credit card information, banking account details, delivery details) or desired by the e-business partner: collecting customer data that later may be analyzed, shared with other businesses or even be sold..

Addressing the requirements from a structural point of view, an efficient framework for preserving security in information systems comprises actions that are categorized as legal, technical, organizational and social. This entails the protection of copyrights for literary, musical, dramatic, and artistic works, as well as of sound recordings, films, broadcasts, and cable programs.. National legislation for the protection of intellectual property rights exists mostly everywhere. At an international level, most prominent role is played by the World Intellectual Property Organization – WIPO (www.wipo.org) who is also administering a total of 23 relevant international treaties. Similar is the situation with the protection of trademarks and patents. (P.T.Joseph 2008, S.Kima 2010)[6,7].

The protection of the right to free speech against the need to control offensive, illegal and potentially dangerous information. This includes the issue of controlling spam. However, it is not always straightforward to apply laws and regulations developed for such a setting in an e-commerce environment.(S.Kima 2010)[7]

Customer (clients) need to be sure that:-
1- They are communicating with the correct server.

2- What they send is delivered unmodified.
3- They can prove that they sent the message
4- Only the author could have written the message.
5- They acknowledge receipt of the message.

All of the concerns listed above can be resolved using some combination of cryptographic method, and certificates methods.

1.6 Security Risks

This type of risks involved resulting from inadequate security is:

1- Bugs or miss-configuration problems in the web sever that can cause the theft of confidential documents

2- Risks on the Browsers' side i.e. breach of user's privacy, damage of user's system, crash the browser etc

3- Interception of data sent from browser to sever or vice versa. This is possible at any point on the pathway between browser and the server i.e. network on browser's side, network on server's side, end user's ISP (Internet Service Provider), the server ISP or either ISP's regional access.(P.T.Joseph 2008).

1.7 The Psychological Aspect of Security

The psychological aspect of security incorporates the feeling of fear, the need to feel that one's money is secure, and the ability to control the payment process and performance of online transactions. Many customers have the misconception that the use of e-commerce for buying and selling is vulnerable and that there is a high probability that their money will be lost. This is due to the intrinsic nature of e commerce, being remote rather than face-to -face. Therefore, the user does not touch or see anything except the computer screen; what lies behind this screen is unknown, and this makes consumers very skeptical .

1.8 Cooperative Responsibility

Cooperative responsibility means that the success of e-commerce in terms of security involves the responsibility of different actors who complement each other rather than a single responsibility. Security conditions Part of this responsibility lies in management's commitment to the necessary expenditure on security. Websites that present such information to their users so that they can verify it before conducting their transactions encourage users to feel that the companies are committed to their customer's security. The government can play a major role in e-caned accountable for security violations. It is the education system's responsibility to increase individual awareness and perception by enriching people's knowledge and experience of security and the use of ecommerce as well as propagating a culture of using eservices to carry out activities online. (J.Rees, 2003)[8]

1.9 Polices of E-commerce security measure

There are different policies used to ensure and measure security in E-commerce environment, we shall explain some of them in the following sections, which are: Privacy, Cryptography, and certificates.

1.9.1 Privacy policy

According to a study released by commerce "Net & Nielsen Media Research", More than 2 out of every five people in North America are now Internet users and the web is becoming as integral part of daily life Without a through privacy security policy, it's not possible to spend money in a responsible and cost – effective manner. Develop a privacy security policy that includes defining the sensitivity of information, the exposure of the organization if that information was likelihood of those risks becoming reality. Privacy polices architecture the manner in which a company collects, uses, protects data, and the choices they offer consumers to exercise rights when their personal information is used. The basis of this policy, consumers can determine whether and to what extent they wish to make information available to companies. (Donini V, 2006)[9]

1.9.2 Cryptography

1- Secrete key cipher system.
2- Public-key cipher system

1.9.2.1 Secrete Key:

Secret key cryptography is the oldest type of method in which to write things in secret. There are tow main type of Cipher systems are classified into 2 classes which are:-

Secrete key cryptography, transposition and substitution. Transposition cipher encrypt the original message by changing characters order in which they occurred. Where as in substitution cipher, the original message was encrypted by replacing there characters with other characters. In both types, both the sender and receiver share the same secret keys. The most widely used secret key scheme today is called Data Encryption Standard (DES). DES cipher work with 56-bit secret key and 16 rounds to transform a block of plaintext into chiper text.

1.9.2.2 Public Key:

Public-key cryptography was developed to solve the secret-key distribution problem associated with secrete key method. It was first publicly described in 1976 by Stanford University Professor Martin Hellman and graduate student Whitfield Diffie. Public key method use tows different but mathematically related, keys. One of the keys is used to encrypt the data, i.e. plaintext and the second key is used to decrypt the cipher text .The second problem that Daffier pondered, and one that was apparently unrelated to the first was that of "digital signatures". Rivest Shamir-Adleman (RSA) scheme is the most widely accepted and implemented general-purpose approach to public-key encryption. The RSA scheme is a block cipher in which the plaintext and cipher text are integers between 0 and n-1 for some n. A typical size of n is 1024 bits or 309 decimal digits. The block size must be less than or equal to log2 (n). Encryption and decryption are of the following form for some plaintext M, and cipher text C:

C= M ^e mod n

M= C^d mod n = (M^e)^d mod n = M ^ ed mod n

Both sender and receiver must know the value of n. The sender knows the value of e and only the receiver knows the values of d. Thus, this is a public-key encryption algorithm with a public key of KU= {e,n},

and a private key of KR={d,n}

1.9.3 Certificate:-

Certificates bind identity, authority, public key, and the other information to a user. For most internet E-commerce application, certificates using a format defined in international telecommunication union telecommunication standardization sector (ITU-T). Recommendation X.509 is employed. An X.509 certificate contains such information as the:

1- Certificate holder's name and identifier.
2- Certificate holder's public key information.
3- Key usage limitation definition.
4- Certificate policy information.
5- Certificate issuer's name and id.

1.10 Pretty Good Privacy (PGP) :-

PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications. PGP has grown explosively and is now widely used, three main reasons can be cited for this growth: First: It is based on algorithm that has survived extensive public review and are considered extremely secure. Second: It has a wide range of applicability. The actual operation of PGP consists of five services: authentication, confidentiality, compression, e-mail compatibility and segmentation. In the following sections we examine the first two services since they are highly concern with this paper aim that is e-commerce security.

1.10.1 Authentication :

Authentication requires a digital signature. The process begins with a mathematical summary called a "hash", which acts as a "Fingerprint" of the message. The message contents cannot be changed without altering the has code. This hash code is then encrypted with sender's private key and attached to the message. When the message has been received, the hash code attached to the message is compared to another hash code or summary calculated by the recipient. I Keys for digital signatures are filed in a public-key directory, made up of "certificates" for every user. The digital signature scheme done in the following sequence:

- The sender creates a message. - SHA-1 hashing code is used to generate a 160-bit hash code of the message.
- The hash code is encrypted with RSA using the sender's private key, and the result is prep ended to the message.
- The receiver uses RSA with the sender's public key to decrypt and recover the - The receiver generates a new hash code for the message and compares it with the decrypted hash code. If the two match, the message is accepted as authentic.

1.10.2 Confidentiality :-

Confidentiality is provided by encrypting message to be transmitted or to be stored locally as files as described in the following sequences, see figure 1:

- The sender generates a message and a random 128-bit number to be used as a session key for this message only.
- The message is encrypted, with session key.
-The session key is encrypted with RSA, using the recipient's public key, and is prep ended to the message.
- The receiver uses RSA with its private key to decrypt and recover the session key.
- The session key is used to decrypt the message.

Te last three PGP services : Compression : A message may be compressed using ZIP. E-mail compatibility: An encrypted message may be converted to an ASCII string by using some conversion algorithm to provide transparency for E-commerce. Segmentation's accommodate maximum message size limitations, PGP perform segmentation.

1.11 Secure Communication Protocol:-

The safety of payment system is the key element of EC. Currently the key technology to ensure the safety of system is as follows: Security Socket Layer (SSL) and safety electronic transaction, which are mainly two kinds of important communication protocols, either of which can offer a method of reliable payment through internet. Several kinds of coding protocols are in use on Internet, every layer of the corresponding seven layers of the network modes has its relevant protocol. For instance, we have application layer of SET protocol, and session layer of SSL protocol. Among all the protocols, SSL and SET have the closest relation with EC.

1.11.1 Security Socket Layer protocol SSL

SSL is the protocol that encodes the whole session among computers and provides the safe communication service on Internet. It is widely used among sensitive information concerning capital balancing. Two kinds of coding are used in SSL:

1.Public coding key is used in process of connection.
2. Special coding key is used in process of session.

The type and intensification of encoding are different according to the declaration made during the process of connection of two ends.

SSL provide the safe connection between two computers. The payment system is always constructed by way of transmitting credit card number through SSL connection; the bank of network and other financing payment system is constructed on SSL as well. Though the EC development is accumulated by credit payment under base of SSL, yet more advanced technology of payment system should be adopted to make the EC spread its area more broadly.

1.11.2 Secure Electronic Transaction SET

SET protocol aims to offer a solution for business by way of credit card payment among the customer, the supplier and the bank. Many parts are included in the SET, to meet the need of problem solving at different stage in business. SET was developed by international organizations of Visa and MasterCard and now it has won support from many large internal companies like IBM, HP, Microsoft, Netscape, VeriFone, GTE, Terisa and VeriSign, etc.

(1) Ensure the confidentiality of information and avoid being wiretapped when information is transmitted on line. Only the authorized legal person can get and decode the information;

(2) Ensure the entity of payment information, secure the data transmitted can be received fully without any alteration in the middle way.

(3) Attest the supplier and the customer, verify the validity of supplier, card holder and business activity which do business on the public network;

(4) Secure wide mutual operationally, ensure the communication protocol, message formatting and standard being adopted have the common adaptability. Thus various products of different supplier can be integrated on public interlinking networks.

SET protocol is more complex than SSL protocol, for by SET not only single session between two ends can be coded, but also multi-session among multi-ends can be coded and recognized. Three stages are included in the SET trade:-

(1) In the inquiry stage, customer and supplier confirm the detailed information on the payment method.

(2) In the confirming stage of payment, the suppliers will confirm with the bank, they will get the payment as the trading proceeds.

(3) In the money-accepting stage, the suppliers will bring forth all the detailed information concerning all the relevant trading to the bank, and the bank will transfer the payment for goods in a proper way.

(4) A customer only has relation with the first stage, bank has relation with the second stage and third stage, while a supplier has relation with all the three stages and every stage is involved in the data coding technology and digital signature by RSA.

1.12 Weak password v\s strong password:-

- **Week password** :-
- In week password the password is the simple name of any person and industry or any other management like as:-
- user name kuldeep
- password chahal
- The week security password is easily destroyed by any hacker
- **Strong password** :-
- In the strong password the special symbols like (34&^3%) is used instead of the simple name of a person.
- User Name kuldeep
- password 23% 67&

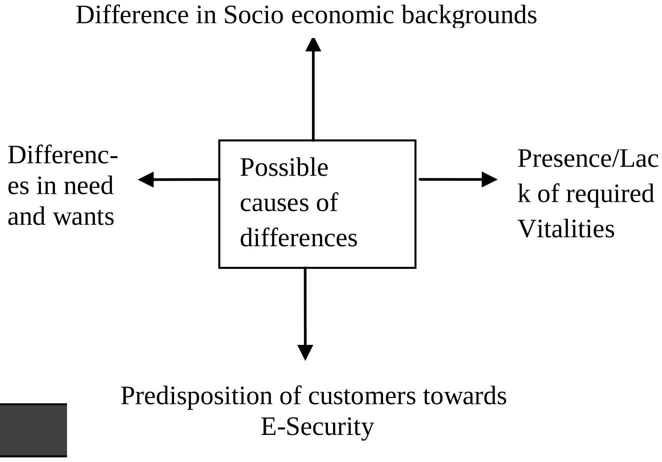
The strong password is not easily remembered and distorted by hackers.

1.13 Objectives of Study:-

1) To protect vital information:-
2) To achieve privacy by using Encryption and Decryption techniques.
3) To identify Authentication:-
4) To Identify Encryption /Decryption of message:-
5) To Improved Integrity of data:-
6) To Provide Secure Electronic payment system:-

II. PROBLEM FORMULATION

Despite different types of relationship between Banking system and security. I want to distinguish here security in banks. I studied here how can we save our account balance in bank system by implementing the security through an account no. in any bank.


Difference in Socio economic backgrounds
Differenc-es in need and wants
Possible causes of differences
Presence/Lack of required Vitalities
Predisposition of customers towards E-Security

III. RESEARCH METHODOLOGY

This studied have been carried out on online banking. Data used in this study collected basically from the secondary sources. Primary data also collected through personal interview method conducting the person who is supposed to have knowledge about the topic. Secondary data have been collected from various sources including websites, newspapers, various published and unpublished article about pre-primary education etc.

3.1Survey Instrument:-

A sample of some respondents from branches of e-security was selected according to connivance. Some materials have collected from books, journals etc. The information is based on different web site resource.

The study is like as a project that is implement to provide security in banking management system. The security is implemented through the account no. in any bank. Security is provided by giving unique account no. to each customer. To develop software for E-banking security the information is collected from many branches

3.2 Collection of data through questionnaire :-

- In this method a questionnaire is sent to the person concerned with request to answer the questions and return the questionnaire. A questionnaire consists of a number of questions printed or typed in a definite order on a form or set of forms. The questionnaire is mailed to respondent who are expected to read and understand the question The and write down the reply in the space meant for the purpose in questionnaire itself. The respondent to have answer the questions on their own.

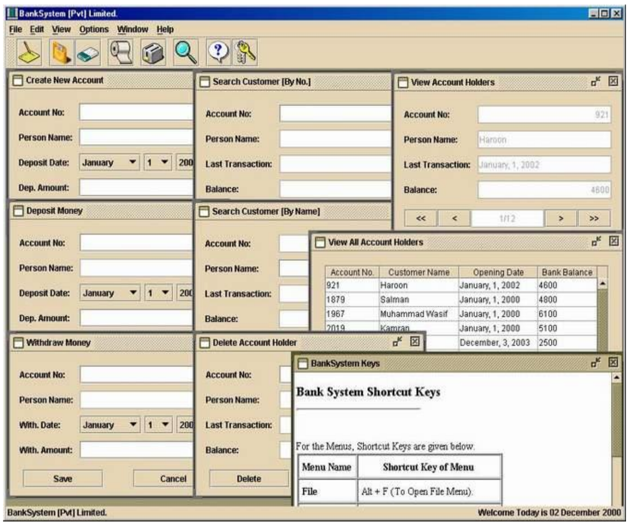
The research methodology on E-Commerce Security is based on the survey .The objective type questions have been designed in the survey .Some responses have been collected from different people. Like (student, Professional and others). The result of survey shown in graphs

3.3 Result

This is a descriptive research which has studied the present conditions. The relevant data was collected based on e-commerce privacy security System ,which most suitable for increasing security in e-commerce.

IV. DATA INTERPRETATION

Project of Security in E-Banking



Account No: 921
Person Name: Haroon
Last Transaction: January, 1, 2002
Balance: 4600
<< < 1/12 > >>

Account No.	Customer Name	Opening Date	Bank Balance
921	Haroon	January, 1, 2002	4600
1879	Salman	January, 1, 2000	4800
1967	Muhammad Wasif	January, 1, 2000	6100
2019	Kamran	January, 1, 2000	5100
		December, 3, 2003	2500

Bank System Shortcut Keys

For the Menus, Shortcut Keys are given below.

Menu Name	Shortcut Key of Menu
File	Alt + F (To Open File Menu).

Overview

This Program is for those who not only want to keep their Records
but they want to keep their Bank Balance updated too. This is the
Best Program for them. It is very easy to use as it is totaly GUI
[Graphical User Interface] based application.

System Requirements

To Use Mubarik Arts System You must Need The Following
1 :- Pentium II OR Higher
2 :- Java Development Kit 1.2 [1.3 Recommended]
3 :- MS WINDOWS 98 OR Higher
4 :- 64MB Ram [128MB Recommended]
5 :- VJA [A Good Company VGA So Programs Interface Show Nicely]

How To Run

It is easy to Run Bank-System. Just set path of your Java Folder
in Dos Prompt and then type "Java Bank-System" and press Enter Key.
(I've made this Program on MS-Windows 98 and it works very nicely on
it). If You Face any Problem Then Contact to Author of Bank-System.

Caution

While trying to close the active form it may throw an exception
if u r using java 1.2. Print option of the Bank-System work nice

& quick if Printer attach with the same computer on which Program
is running otherwise it may take a while.

In this study the security is implemented in e-banking system. In this E-banking security system software the account no. of a customer is used as a security issue. The bank can access each customer's Account. But a customer cannot access other customer's because account no. of a customer is a personal security password for accessing E-banking system.

Create New Account:-The customer's account no. is given in numerical characters (10003) and person name is given in alphabetical characters. If a customer give password in alphabetical characters than this E-banking security system software is not allowed to create new account in this software and to access other person's account balance.

Search Customer:- The customer can be find out by using two ways:-

-To search the customer by using his account number.

-To search the customer by using his person name.

Delete Account Holder:- The Account Holder will be easily deleted by using a customer's Account no. and person name.

In this Software the account no of a customer is used as a security code for saving the customer's account balance. If one option in this software is left, That is not allowed for accessing customer's account. This software save customer's Account for a long time.

4.1Observation and Finding

A survey was conducted on E-commerce privacy and security system so as to collect views of different people (student, professional and others). The objective of this survey is to obtain the knowledge of e-commerce privacy and security system prevalent among the users. The responses of people have been represented through graphs and tables on the basis of responses obtained from people. The graphs of questionnaire along with their explanation have been discussed below:-

S.No.	Questions	Yes	No
1	Is E-commerce security critical	40	10
2	Are Consumer communicating With correct server	38	12
3	Is privacy can achieved by using encryption decryption techniques	44	6
4	Do banks provide secure banking service	48	2

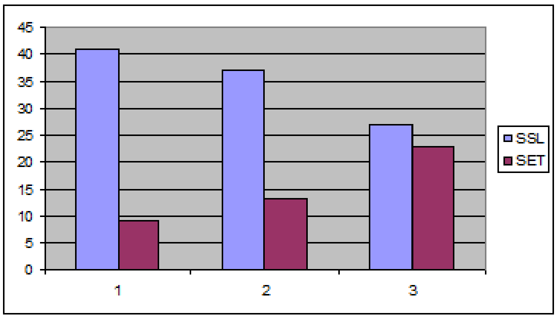


Fig 4.1.1:- Graph Represented Yes/No options: Fig 4.1.1

The graph reveals the following results:-

(1)In this graph the minimum responses of people have been given to the question no. 3 "Can privacy can achieved by using encryption and decryption techniques?" 38 persons were affirmations and 12 persons were negations but in reality the Encryption /decryption techniques are play a great role to achieve privacy . This technique is the best way to take our information private.

(2)In this graph maximum responses are given by peoples to question "Bank provides secure banking services?" 48 responses were in affirmation and 2 responses were in negation. Each Bank can provide security to customers to secure their account in banks. Each bank wants to increased\enhanced its own banks branch so it provides more than more security to increase the satisfaction of people about its bank branch.

S.No.	Questions	SSL	SET
5	In which communication protocol the Web server sends its public key with its certificate	41	9
6	Which Is more complex Protocol	37	13
7	Which security protocol is used to secure electronic payment system	27	23

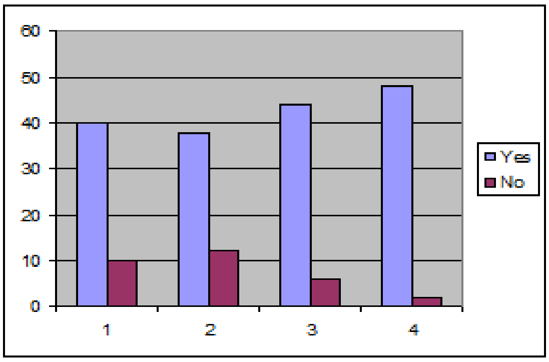
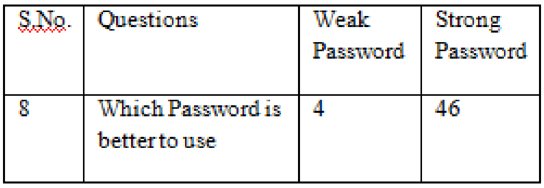


Fig 4.2:- Graph Represented SSL /SET options: Fig 4.2

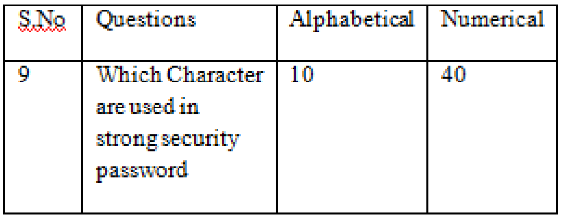
This graph have been connected to show the satisfaction of people for SSL and SET for question no. 5 to 7. The graph reveals following results:-

(1) The maximum people (41) were satisfied with SSL in question no. 5. But some people (9) were not satisfied with it. But in real in SSL protocol the web server sends its public key with its certificate to transfer money and information the right client.

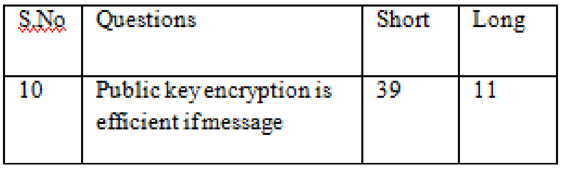
(2) The minimum people (37) were satisfied with SET protocol in question no. 6. But in real words the SET protocol is more complex than SSL protocol. Because SSL is a single session between two ends and in SET is multi-session among multi ends can be coded and recognized.



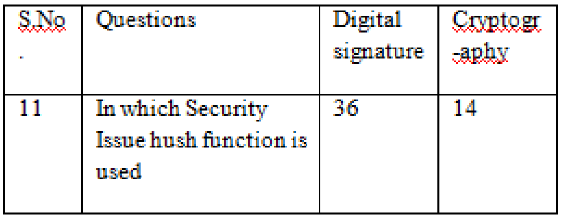
S.No.	Questions	Weak Password	Strong Password
8	Which Password is better to use	4	46



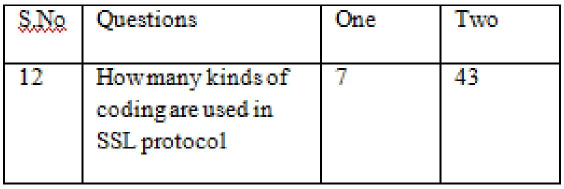
S.No	Questions	Alphabetical	Numerical
9	Which Character are used in strong security password	10	40



S.No	Questions	Short	Long
10	Public key encryption is efficient if message	39	11

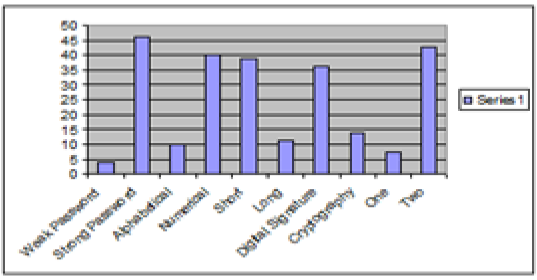


S.No .	Questions	Digital signature	Cryptogr -aphy
11	In which Security Issue hush function is used	36	14



S.No	Questions	One	Two
12	How many kinds of coding are used in SSL protocol	7	43

Fig 4.3:- Graph Represented Ten Options:



This graph identify Ten options (weak password, strong password, Alphabetical, Numerical, short, Long, Digital Signature, Cryptography, One, Two).

(1)The minimum 4 persons were satisfied with weak password and maximum 46 persons were satisfied with strong password in question no.8. Because in strong password numerical characters are used. The numerical character s are not easily remembered so hacker and other persons cannot destroyed it.

(2)40 persons were satisfied with numerical characters and 10 persons were satisfied with Alphabetical characters to question no. 9.

(3)39 persons were satisfied with short message and 11 persons were satisfied with long message in question no. 10. Because short message is easily encrypted by using public key encryption. Hush function is used in digital signature because hush is a digital sign of a person which is used for verification. Some people are give response in other option cryptography is used hush function that is wrong because in cryptography encryption decryption technique are used by using client server's public key or secret key.

(4)7 persons were satisfied with One kind of coding and 43 persons were satisfied with two kind of coding is used in SSL protocol. In real words two type of coding are used in SSL communication protocol. That is as follow:-

- Public Key
- Special Key

Public coding key is used in process of connection. Special coding key is used in process of session

S.No.	Questions	Satisfied	Unsatisfied	Neutral
13	Do avoid you reusing the same user id and password at multiple website	29	12	9
14	Do biometrics allow easy, fast and more Secure authentication	31	3	16
15	To spend money in a responsible and cost effective manner without privacy security policy is not possible	31	7	12
16	Can bank a provide security by using unique account number	40	3	7
17	Is our account balance is safe in banks by using security protocol	39	1	10
18	Is your important information is protected	39	0	11
19	Payment is securely transferred from one account to another	34	2	14

Fig.4.4:-Graph Represented Satisfied/Unsatisfied/ Neutral Options:

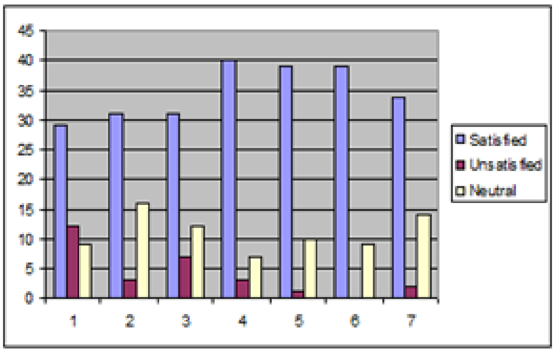


Fig 4.4

This graph indicated three options (Satisfied, Unsatisfied, Neutral). The graph revels following results:-

(1) 40 persons answered in satisfied, 3 persons respondent unsatisfied and 7 persons respondent in neutral to question no. 16. Because these peoples are satisfied with that a bank can provide security by giving unique account no. to each bank.

(2) 39 persons answered in satisfied, 0 persons respondent unsatisfied and 11 persons respondent in neutral to question 18.

(3) 34 persons answered in satisfied, 2 persons respondent unsatisfied and 14 persons respondent in neutral to question no. 19. SSL and SET communication protocols are used to provide secure electronic payment system. But in some times the balance is not securely transferred from one account to another account .So some peoples are neutral in this question.

Fig.4.5:- Overall Analysis of Security System

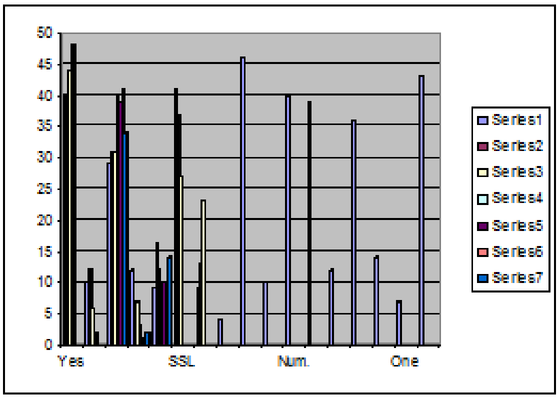


Fig 4.5 Overall Analysis

V. CONCLUSION & FUTURE SCOP

5.1 Conclusions:-

In banks all the functions and activities are safe by using security issues. In this research in banking management. Open account and check the balance and do any transaction and delete any account very securely if we know the password of any customer.

The main feature of the research that the data is safe in banking management for long time and open any account after a long time and . This secure banking system software is access only by the bank (pvt.) and by customer. A customer cannot access the other customer's account in e-bank system. Strong password is used to secure bank account of any customer instead of weak password because strong password is not easily remembered and used. Feedback can be obtained easily as internet is virtual in nature. Customer loyalty can be gain. Personal attention can be given by bank to customer also quality service can be served.

Some study have been designed on survey .The respondent have to answer the questions on their own. Some people satisfies own our views. But some peoples were not satisfies with us. Respondents have adequate time to give well through out answers.

5.2 Future Scope

In e-banking security system SSL and SET (Secure Socket Layer and Safely electronic transaction) communication protocols are used .

- SSL and SET solve the safety problem in electronic payment of credit card .They ensure the confidentially of information.
- But in future biometric measure is used in banks to safe banking management system.
- The biometric measure is also used on debit cards of each bank to safe card holders account balance.
- Reduce deployment costs and distribute information easily.
- The Future scope of the study of Security is use to reduce threats.
- Security is used in the long run results in reduction of number of branches, saying rentals of related buildings and properties.
- By using Security issues wages and salary bill of banks get reduced Online banking convenience of client has considerably increased as the can transact from home or office.

If the better security operate than net banking and e- marketing will be increase.

REFERENCE

[1] Kaur M, "*E-Commerce Kalyani Publictaion*" , Delhi (2012)

[2] Corbitt,B.J. ," *Trust and e-commerce a study of e-commerce perceptions*", Electronic Commerce Research & Application, Vol .2 No.3 ,pp.203 -15(2003)

[3] Aladwani.A," *Key Internet Characteristics and e-commerce issues In Arab Countries*", Information Technology and People ,Vol 16,1:9-20(2003)

[4] Sharma A & Yurcik.W , " *A study of e- filinr tax websites contrasting security techniques versus security perception* ", proceedings of the Tenth Americas conference on information system , New york , 2004

[5] Kim C," *An empirical study of customers perceptions of security and trust in e-payment system*", Electronic commerce research and applications , Volume 9. Number 1, pp .84-95(2010)

[6] Joseph P.T, S.J(2008)," *An Indian perspective*", 3rd edition, E-Commerce,by PHI learning private limited.

[7] Kima S ," *An Empirical Study of Customers perceptions of security and trust in e-payment system*," Electronic Commerce research and applications, Vol .9 No. 1 pp.84-95(2010)

[8] Rees.J , Bandyopandhayoy.S and Spafford.E, "*policy framework for interpreting risk in E- commerce security* ",communications of the ACM, vol . 46, no. 7, 2003

[10] www.wikipedia.com