7th International Conference on Recent Trends in Engineering, Science & Management
Genba Sopanrao Moze College of Engineering, Balewadi-Baner, Pune (ICRTESM-17)
01st-2nd April 2017, www.conferenceworld.in ISBN: 978-93-86171-12-2

TRACKING UNAUTHORIZED USER ACCESS IN BANKING SYSTEM

Priya Kitukale

M.tech Student, Department of CSE, Jhulelal Institute of Technology, Nagpur, India

ABSTRACT

In this paper a honey pot security system is use to protected all e-transactions web site there is currently present system is standalone system(desktop system) which is made up in java language. This system is protected desktop files when we protect a particular file and when unauthorized user try to access a protected files a present system trap all related information of unauthorized user and send detail report to admin of a system. After successful performances of e-banking web site we created an intruder attack trapping system. A system which trap all intruder activity which try to access an e-banking services unauthentic ally. Our system identify a intruder activity created intruder activity report and send that report to admin for further operation. If some time intruder gets success to access a system that time our system divert an intruder access root to dummy root. Some time there is a more traffic over a network our provided solution to solve a network traffic problem and divert an irregular user to other root and after some time network traffic is became normal our system gets that user again in a same track. So our system is provided security to all e-banking system to perform a secured transaction and our system can identified intruder activity and try to avoid their unauthorized access.

Keywords - HD 40 GB, internet information server, MS SQL server express edition, RAM 500MB, visual studio 2005, windows XP.

I. INTRODUCTION

Basically present system is standalone system it is use to protected or trap an unauthorized user activity. Now a proposed system is global web base system .Here we use a asp.net services and application to implement a honey pot system. Honey pot system is provided security services to banking web site where lot of E-transaction is perform. So our honey pot system is totally base upon banking system and provided various way to stop all kind of intruder attack. Here we created one banking web site which provided all internet banking services. Now our banking system is provided all banking services like here a register customer can perform a virtual money transaction. To providing access to a customer which may or may not be valid that all customer authenticated by our system. So our banking site full fills all customer internets banking needs. The results also show that privacy and security concerns are the main impediment to shopping on the Internet. The implication is that the successful organizations will be those who expend their resources and efforts to ensure that IT users' concerns are adequately addressed.

II. WHAT IS HONEYPOT

IP computer terminology a honey pot is computer security mechanism set to detect deflector in some manner, counteract attempts at unauthorized use of information systems .generally a honeypot consist of data (for example in network site) that appear to be legitimate part of the site but is actually isolated and monitored and that seems to content information or a resource of value to attackers .which are then blocked .this is similar to the police baiting a criminal and then conducting undercover surveillance and finally punishing the criminal.

Honeypot systems are not used neither detecting intrusion detection system nor the firewall for a direct specific problem. Honeypots are used as a part of security systems and what kind of problem they will offer solution is depends on the design and usage purposes. Hence to the contrary other information security equipment's it is not to be able to mention a honeypot that is able to give a general answer to every problem solution. In technical literature there are various security applications like intrusion detection and prevention (IDPS) are used collectively.

Many different approaches to building detection models have been proposed. A survey and comparison of detection techniques is given in this paper presents an approach for modeling normal sequences using look ahead pairs and contiguous sequences. This paper presents a statistical method to determine sequences which occur more frequently in intrusion data as opposed to normal data. This paper uses neural networks to model normal data and examines unlabeled data for anomaly detection by looking at user profiles and comparing the activity during an intrusion to the activity under normal use.

2.1 Problem Definition

In old system the new threats are constantly emerging, Firewall and VPN fail to prevent all intrusions in system, Network intrusion detection systems (NIDS) or Intrusion, Detection Systems (IDS) are effective means of detecting attacks. The increasing quantity and diversity of legitimate network traffic. NIDS are unable to detect new forms of attacks. We proposed a secure system for banking application using Honey pots. Using this system data integrity can be ensured along with monitoring the interaction to detect possible attack.

2.2 Overview of the present working system

The attacker uses his own techniques to get into the system to get some important information or data. There will be two kinds of interactions. First, low interaction honey pots, in which enough interaction is provided to attackers, through which, some interested attacks may be known to the system. Second, high interaction honey pots, in which through full interaction with the attacker, detail information is known.

It will basically segregate data into three layers i.e. namely user interface (open source),the dummy programs (to lure the attackers and to keep into system busy to help us to take steps) and the main part of the system. Along with the intruder detection it will also make us able to track them down as there will be an inbuilt system to maintain their data. The other users will access the user interface (UI) which will be an open source.

It will be followed by the layer of dummy programs which will be hidden from the actual UI, but the attackers can reach it easily. These programs will take a lot of time as it will create a delay and in the meantime the system will raise an alarm that will inform the system administrator that there is an intrusion going on

and will give the respective authority the necessary time to take according actions. Also there will be a tracking program that will track the attackers and will help in getting hold over him. The system will keep track of the changes the attacker's make on the dummy data generated by the underlying dummy programs so as to make us aware of the manipulations the attackers were to make to the original data if it had been reachable, and also will help in taking necessary decisions as what part of the database is more crucial for it was attacked and need the almost care and protection from future threads. The final layer that is the main database of interest will be most preciously protected can be accessed only with the password of administrator.

III. PROPOSED SYSTEM

In this paper the solution for the creation of new systems which provides procedural details for implementing the system. It goes through logical and physical design which emphasis on the preparing I/O specification, preparing control specification, specifying the implementation plant, preparing a logical design, designing the O/P forms.

Before we implement in the software, the steps to be followed are drawing the flowchart of drawing the flow diagrams, building databases, coding the software with respective language and the database, designing the software with respect to user's requirements, prototyping the software and lastly making the planning and documentation.

3.1 Entity Relationship Diagram

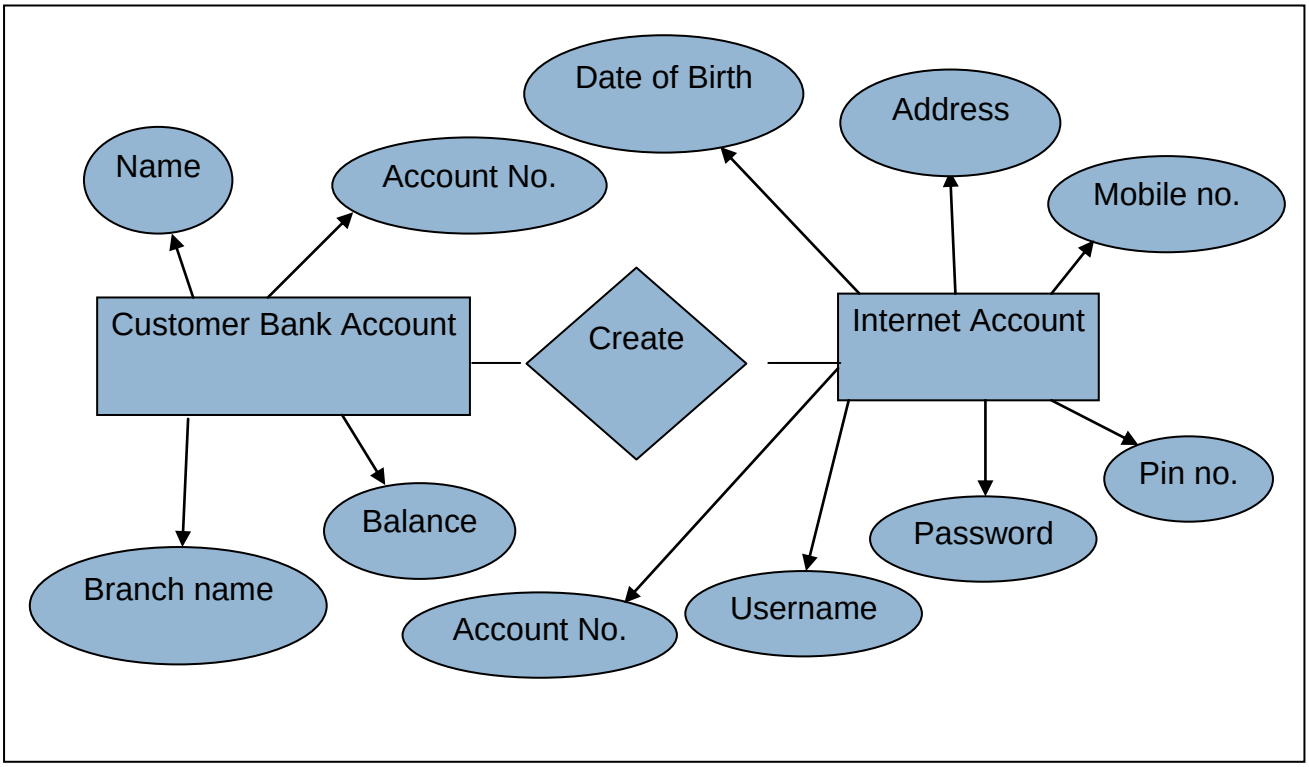

Figure 1.

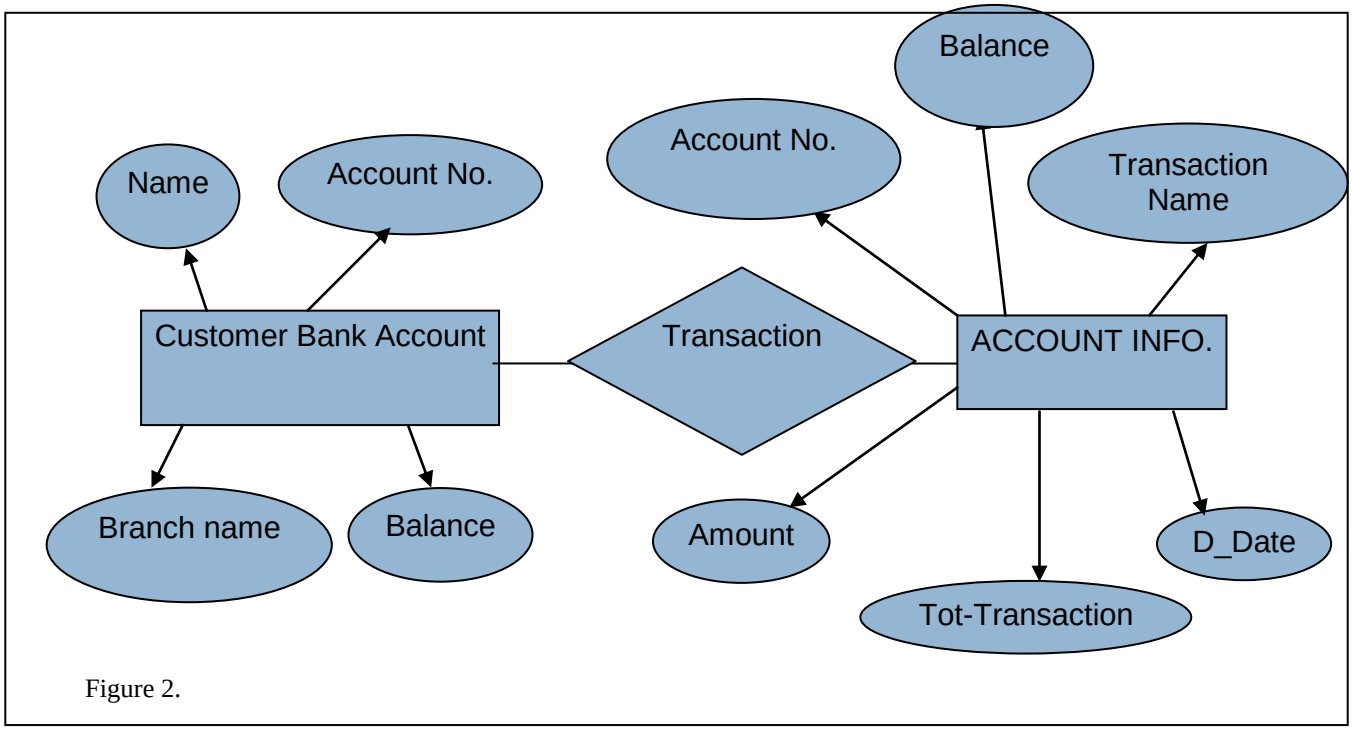

Figure 2.

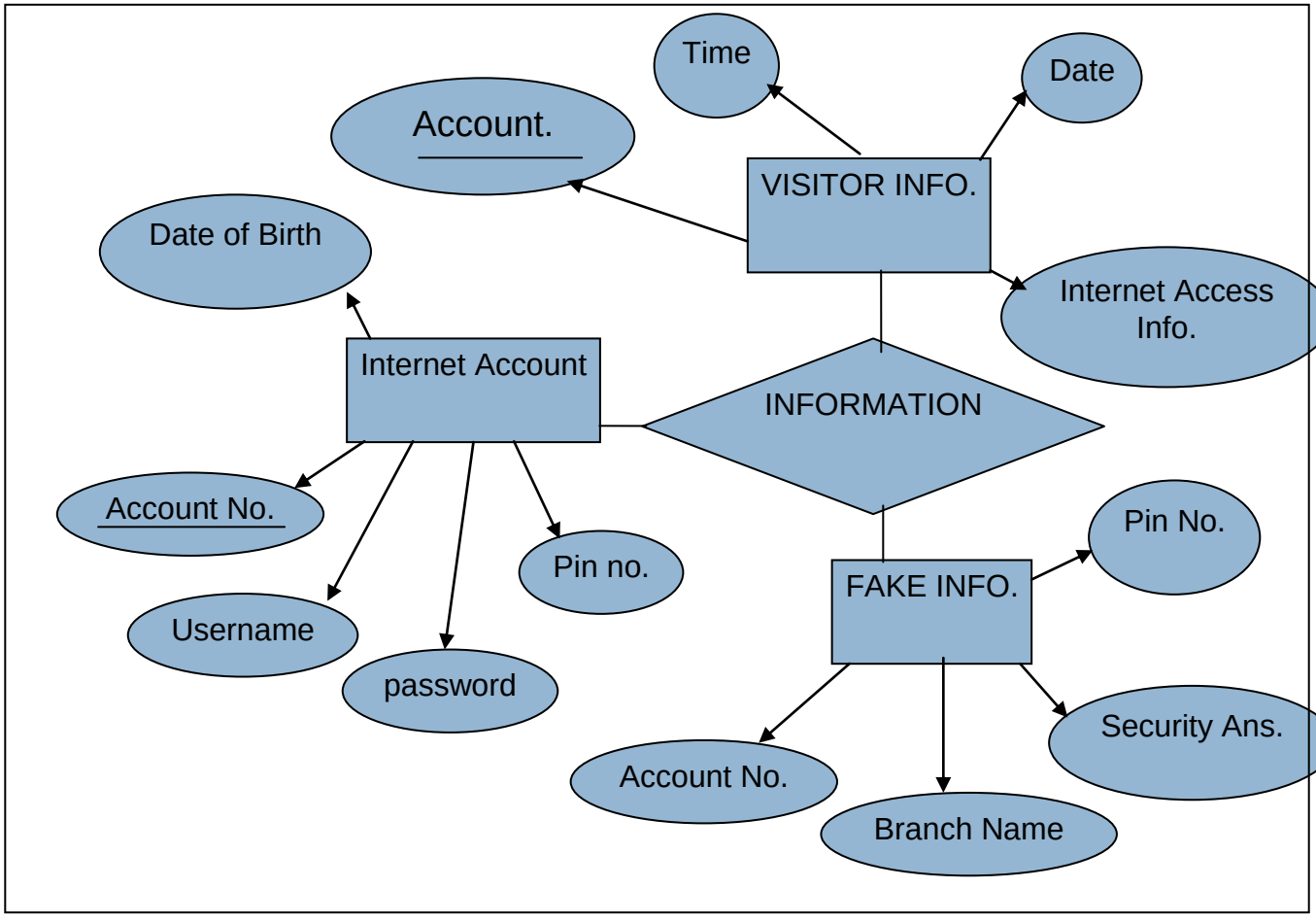

Figure 3.

ISBN: 978-93-86171-12-2

3.2 Database Design

This part consists of information about database. It consists of what type of database is used to develop paper and how it is maintained and also what information does the database stores.

3.3 Schema Design

Our paper is proposed to manage all the aspects related with Honey-Pot. We have included only one database which keeps the record of Customer. The database in our system is implemented using the sql server 2005. Information can be modified within the same file according to necessity.

3.3.1 Database Dictionary

Table 1: Registration form

FIELD NAME	DATA TYPE	DESCRIPTION	CONSTRAINTS
Acc_no	int	Stores acc no	Primary Key
Name	char(10)	Use to store name	Not Null
Surname	char(10)	Use to store surname	Not Null
Date of birth	varchar(50)	Use to store dob	Null
Emailed	varchar(50)	Use to store email	Null
Address	varChar(50)	Use to store address	Null
City	char(20)	Use to store city	Null
State	char(20)	Use to store state	Null
Country	Char(20)	Use to store country	Null
Username	Varchar(50)	Use to store username	Not null
Password	Varchar(50)	Use to store password	Not null
Account open	Varchar(10)	Use to account	Not null
Security	Varchar(100)	Use to store security question	Not null
Answer	Varchar(50)	Use to store answer	Not null
Branch name	Varchar(50)	Use to store brabch name	Not null
Mobile no	Varchar(50)	Use to store no	Null
Gender	Char(10)	Use to store gender	null

Table 2: Field officer

FIELD NAME	DATA TYPE	DESCRIPTION	CONSTRAINTS
Acc_no	Int	Stores acc no	Primary Key
Name	char(10)	Use to store name	Not Null
Surname	char(10)	Use to store surname	Not Null
Date of birth	varchar(50)	Use to store dob	Null
Emailed	varchar(50)	Use to store email	Null
Address	varChar(50)	Use to store address	Null
City	char(20)	Use to store city	Null
State	char(20)	Use to store state	Null
Country	Char(20)	Use to store country	Null
Branch name	Varchar(50)	Use to store branch name	Not null
Mobile no	Varchar(50)	Use to store no	null
Gender	Char(10)	Use to store gender	Null
Net income	Bigint	Use to store income	Not Null
Car_loan	Bigint	Use to store loan	Not Null
Loan date	Varchar(50)	Use to store date	Not null
Interest loan	Bigint	Use to store interest	Not null
Emi	Bigint	Use to store emi	Not null
Total	Bigint	Use to store total	Not null
Cif_no	Char(10)	Use to store cif	Not null

Table 3: Transaction_car

FIELD NAME	DATA TYPE	DESCRIPTION	CONSTRAINTS
Acc_no	Int	Stores acc no	Primary Key
Name	char(10)	Use to store name	Not Null
Surname	char(10)	Use to store surname	Not Null
Due date	Varchar(50)	Use to store due date	Not null
Emi	Bigint	Use to store emi	Not null
Before total	Bigint	Use to store total before transc	Not null
After total	Bigint	Use to store total before transc	Not null
Deposit	Bigint	Use to store deposit	Not null
Next instalment	Varchar(50)	Use to store instalment	Not null

3.4 Advantages Of The Proposed System

Easy to access from anywhere: So it is web application it can access from anywhere, and customer use his accounts.

Online office work: Employee of the bank work on the online portal which is online connected to the central system of the bank that is all work is stored into the central database.

High Level Security: Honey pot security provides high level of security so that hackers and intruders are not reaching to the original database and system of the ebank.

Illusion of original system: When intruder try to enter the system he has to go through the many 2-3 level of security ,if he unable to pass it he will redirect to the fake system and data which is look like original system, and all tricks used by him will recorded into other database.

Dynamic in nature: An effective system should be largely dynamic taking advantage of technology that automates this process rather than relying on manual processes. Application should serve dynamic user based customized web pages to its clients from server.

IV. SYSTEM DESIGN

Requirement specification of the proposed system is divided in two major modules. First is User modules for application. And second is Honey pot security modules. In our system there are 4 major users each user as one module: Administrator, Internal Users, Customers (Registered users), General users. All the users we describe as follows.

4.1 Honey nets and Honey farms

Honey nets and honey farms are the names given to groups of honey pots. Honey farms tend to be more centralized. Grouping honey pots provide many synergies that help to mitigate many of the deficiencies of traditional honey pots. For instance, honey pots often restrict outbound traffic in order to avoid attacking non-honey pot nodes. However, this restriction allows honey pots to be identified by an attacker. Honey farms as redirection points for outbound traffic from each individual honey pot. These redirection nodes also behave like real victims. Show the redirection of outbound traffic from a honey pot to another node in the honey farm.

An Administrator is the first user module can create an all internal users.It verifies all internal users' activity. Check intruder activity report and using their report administrator take a necessary action.

Internal Users can create by admin. Internal users can handle all banking customer activity (A physical operation or paper work performs by internal user). A banking employee is our internal users.

Customer (Registered Users) user how register him/herself such user is our customer. A user is authorized user which gets proper access in our banking system. A user performs all banking activity like virtual transaction all accesses all other banking services.

General User A user which access an e-banking web site and try to identify all latest services or facility provided by the bank. A user which just access a web site and getting information from e-banking web site called as a general user.

4.2 Operating environment of Realizing document

- *Customer***:** We want an e-banking system with high security level,
- *Developer***:** What type of security system you require?

- *Customer***:** We want a security system which not only blocks the hackers and intruder by entering into the system but also keep track of all tricks of them.
- *Developer***:** For whom you want to develop the system?
- *Customer:* E-banking system for banks customers wish to do online banking and also for *banks* internal user so that they can perform office work online.
- *Developer:* Which kind of system you have now?
- *Customer :* We using a manual system for doing all banking operation.
- *Developer:* How present system working?
- *Customer:* Every customer physically come into bank and accesses their accounts, and *internal* user performs all manipulation offline.
- *Developer:* To which you want to provide this security?
- *Customer:* To the data of all customers related information and access information of the employees of the bank.
- *Developer:* Who will maintain all system work.
- *Customer:* Administrator will manage it, and then branch manager at the internal user.
- *Developer:* What thing we can use to develop new system for office users?
- *Customer:* You can use our worksheets for observing the present working system for *office* users.

4.3 Feasibility Analysis

A feasibility study is defined as an evaluation or analysis of the potential impact of a proposed paper. A feasibility study is conducted to assist decision makers in determining whether or not to implement a particular paper or program. The feasibility study is based on extensive research on both the current practices and the proposed paper. It is an analysis of possible alternative solutions to a problem and a recommendation on a best alternative. Main purpose of the organization is to manage and maintain history of above tasks using less number of resources. Goal of the organization is to complete the task according to timesheet and economically manage the Honey-Pot. A feasibility study is a preliminary study undertaken to determine and document papers viability. The results of this study are used to make a decision whether to proceed with the paper. The system has been tested with following points:

4.3.1 Economic Feasibility Study

Economic analysis is the most frequently used technique for evaluating the effectiveness of the proposed system. It is more commonly known as cost benefit analysis. The study of this type of feasibility determines the benefit that is expected from this Honey-Pot and compares them with the costs incurred. As far as our paper is concerned it involves the various costs such as software costs, maintenance costs and the cost of training the individuals working on this paper but all these still make it cost-effective when we compare it with the existing manual system.

4.3.2 Technical Feasibility Study

Technical feasibility of a system deals with functionality, performance and constraints that affect the system. Technical analysis involves questions such as whether the technology needed for exists, how difficult it will

ISBN: 978-93-86171-12-2

would be too built and whether the firm has enough experience using that technology. Technical feasibility study involves financial considerations to accommodate technical enhancement. In the point of view of our system the computerization of the existing system was need of the hour because the pace at which the work was done in the manual system was very slow and involved less technology and more manpower. Hence the need for technology was on a row which would enable the firms to decrease manpower and increase the work speed.

4.3.3 Operational Feasibility Study

The proposed system will be influential in making the existing system more users friendly and will provide an environment which will enable the users to perform the specified task efficiently. Here are the points to be considered. This proposed system will change the management system. The software that is developed should be in such a way that the user must easily understand the operations. User-friendly screens are to be designed to allow the user to get familiar with the developed software.

4.4 How To Implement

4.4.1 Pre-Implementation

The implementation phase is less creative than the design. To implement our new Payroll system we have to give training to user that how to use this Payroll system. As this proposed system is user friendly it is very easy for user to learn how to use it. There is no need of extensive user training. First user will work on data provided for testing, means he will try to enter, delete, modify and all operation given is our system. If he is successful in it he will allow running "live data".

4.4.2 Post –Implementation

After the installation phase is completed and the user is adjusted to changes created by the candidate system, evaluation and maintained begin. In our new Payroll system less maintains is required. But we have to check the performance of the hardware and software periodically. Again we have to conscious about any virus should not affect the software.

V. CONCLUSION

Tracking Unauthorized User Access In Banking System" is one of the convenient techniques ever and widely liked by the people all over. Our system is only a small implementation of the great one, just trying to the zenith from the depth of the various concepts of the "Software Engineering" and Programming. The development provides lot of knowledge of both the field Software Engineering and practical implementation of ideas, good graphics New emerging hacking techniques in the future can be easily monitored with the help of the Honey pot System. By using Honey pot System in our system we ca effectively stop the hackers from hacking the Banking systems. The main purpose of the Honey pot System is to maintain each and every action performed by the user in the software system and monitor the different types of attacks. By using the Honey pot System in the software systems the level of security improves. In this paper the Honey pot System is applied to the Banking system, in the future if we apply the Honey pot system to any software systems will be more secured.

REFERENCES

[1] Avinandan Mukherjee, Prithwiraj Nath, (2003) "A model of trust in online relationship banking", International Journal of Bank Marketing, Vol. 21 Iss: 1, pp.5 – 15.

[2] Carlos Flavián, Miguel Guinalíu, (2006) "Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site", Industrial Management & Data Systems, Vol. 106 Iss: 5, pp.601 – 620.

[3] Godwin J. Udo, (2001) "Privacy and security concerns as major barriers for e-commerce: a survey study", Information Management & Computer Security, Vol.9 Iss: 4, pp.165 – 174.

[4] J. Computer Network and Information Security, 2012, 10, 63-75 Published Online September 2012 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2012.10.07

[5] http://www.ijcna.org/Manuscripts%5CVolume-2%5CIssue-5%5CVol-2-issue-5-M-01.pdf.

[6] http://interscience.ac.in/URJA/journals/urja_vol1.1/urja_paper22.pdf.

[7] ASP.NET Security (Published March 1st 2010 by Barry Dorran)

[8] System analysis and design (Published February 1st 1985 by Richard D. Irwin)

[9] http://www.symantec.com/connect/articles/guide-different-kinds-honeypots