IMPLEMENTATION OF AN EXPERT SYSTEM FOR THE ENHANCEMENT OF E-COMMERCE SECURITY

[1]NIKITA RANA, [2]SHIVANI DHAR, [3]PRIYANKA JAGDALE, [4]NIKHIL JAVALKAR

[1,2,3,4]University of Pune
Email; nikitarana.0892@gmail.com, shivani.dhar29@gmail.com, priyanka.jagdale23@gmail.com, nikhil.javalkar@gmail.com

Abstract- In the era where E-commerce has reached every doorstep, people are witnessing a convenient, cost-effective and electronic way of shopping for their desired goods and services. The increase in popularity of E-commerce has become directly proportional to the fears related with secure E-commerce transactions. Security is a state of mind wherein its definition varies from person to person. Therefore, provision of security against malicious activities and threats in a versatile E-commerce environment is a must. As an Expert System is a knowledge based self-learning system, through this paper we aim at exploring the advantages of an expert system and incorporating them in an E-commerce model for the enhancement of security. For the purpose of decision making, this paper introduces the concept of Risk Score Calculation for the identification in abnormalities in user's behaviour which can be subject to further investigation.

Keywords- E-Commerce, Expert System, Research, Security.

I. INTRODUCTION

E-commerce is the exchange of information across electronic networks, at any stage in the supply chain, whether within an organization, between businesses, between businesses and consumers, or between the public and private sector, whether paid or unpaid. In 2012, ecommerce sales topped $1 trillion for the first time in history. The reasons for its demand lie in its convenience, less consumption of time, ability to reach global markets, 24hrs service, opportunity to compare prices, opt for cheaper and better quality products, reduction of burden in infrastructure and user friendliness.

Security is nothing but a state of mind i.e. its concept, ideology, definition, reason and prevention is subjective. Owing to its subjective nature providing 100% security against threats present on the internet is an arduous affair.

Although the E-commerce global sales are growing at the rate of more than 19% per year, the amount of trust people are willing to invest in online transactions is still a major concern. This hesitation can be blamed on meagre provision of holistic security against prevailing threats. Security in Ecommerce implies the protection of e-commerce assets from illegal access, use, alteration or destruction yet, among Internet users, 55% think online shopping is the most risky, 54% express concern at releasing credit card details online, 51% say being unable to physically inspect the goods before paying is a main disadvantage and 30% believed that there was a risk from fraudulent suppliers.

Focusing on the trust factor which is extremely vital from consumers' point of view, through this paper we aim to overcome this barrier by implementing an Expert System to provide a permanent solution. This Expert System alongwith the risk score calculation modulewill help to analyse, correlate and decide the risk level associated with an on-going transaction on an E-commerce site. The purpose of using an Expert System is justified by its ability to procure new knowledge with the passage of time and gaining of experience from system traits. In coordination with the functionalities of an Expert System, the feature of risk score calculation based on a set of parameters has been used to differentiate between legitimate and an illegitimate users.

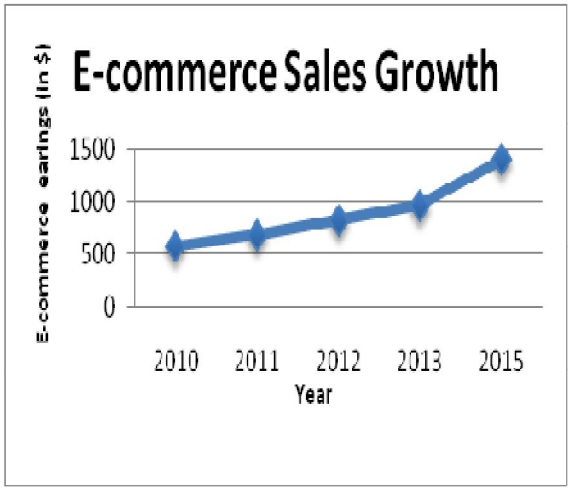

Fig:1.1:Sales Growth

II. SECURITY:

According to the Institute for Security and Open Methodologies.(ISECOM) in the OSSTMM 3, security provides "a form of protection where a separation is created between the assets and the threat." Security is both a feeling and a reality. And

they're not the same. The reality of security is mathematical, based on the probability of different risks and the effectiveness of different countermeasures. That is we can determine how secure a particular website is based on the availability of specific data. Since we are dealing with security over the Internet, it is essential to understand what cyber security encompasses.

Cyber Security: Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction. Essentially, cyber security provides security against various cyber-attacks prevalent in cyber space. These attacks include attacks from Scareware, BOTS, viruses, Trojans, password crackers, keyloggers, malware, SQL injection attacks amongst numerous other attacks.

Due to the existence of these attacks in the internet, E-commerce websites are becoming increasingly vulnerable to cyber threats.E-commerce security covers the six dimensions namely, integrity, non-repudiation, confidentiality, authenticity, privacy and availability. Securing an e-commerce website along all the six dimensions is unfortunately not a foolproof plan of action.

This causes lack of trust that people bestow upon online e-commerce transactions. Thus, this paper mainly focuses on the **TRUST** factor that hampers the success of e-commerce.

Trust is a complex and multifaceted issue that must be addressed from multiple angles. Merely focusing on either Internet and network security applications or web interface alone does not guarantee that consumers will trust e-vendors. Previous research on trust tried to understand consumers' attitudes, intentions, and behaviour that are related to trust in online shopping.

However, it failed to provide a proper solution that can foster online trust because the focus to date is mainly on technical issues and secure transactions rather than what makes consumers trust e-commerce websites.

As B2C e-commerce develops, risks such as identity theft, fraud, phishing, and hacking activities have emerged affecting trust in online shopping. Therefore, the objective of this research is to investigate what factors enhance consumer trust in B2C e-commerce via the Internet.It is now clear that trust and security go hand in hand. The more secure the e-commerce website is the more trust people are willing to invest in e-commerce transactions. As a flipside to this belief, lack of security results in lack of trust. This is evident from the following statistics.

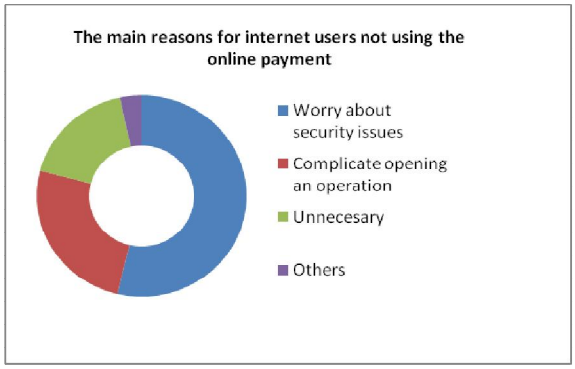

Fig 2.1:Reasons for internet users not using online payment

III. EXPERT SYSTEM

An expert system is a computer program that simulates the judgement and behaviour of a human or an organization that has expert knowledge and experience in a particular field. Typically, such a system contains a knowledge base containing accumulated experience and a set of rules for applying the knowledge base to each particular situation that is described to the program. Sophisticated expert systems can be enhanced with additions to the knowledge base or to the set of rules. An Expert System consists of the following component:

The User Interface: The user interface is the means of communication between a user and the expert systems problem-solving processes. A good expert system is not very useful unless it has an effective interface. It has to be able to accept the queries or instructions in a form that the user enters and translate them into working
instructionsfor the rest of the system

The Knowledge Base: The first part of Knowledge Base takes the input from the outside world through user interface. The source of input can be a book, novel, Newspaper etc. The input is a concept can be divided in to the following categories: substance, quality, action, generality, particularity, inherence and negation and each substance can be earth, water, light, air, ether, time, space, soul and mind as in case of Indian logic.

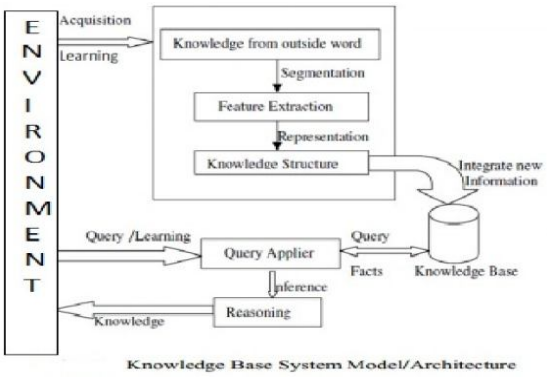

Fig 3.1: Knowledge Base System Model/ Architecture

Knowledge Base consist all the knowledge required to solve the problem. The knowledge base can be general or domain specific.

Inference Engine: An inference engine is a software system that is designed to draw conclusions by analysing problems in light of a database of expert knowledge it draws upon. It reaches logical outcomes based on the premises the data establishes. Sometimes inference engines are also capable of going beyond strict logical processing, and utilize probability calculations to reach conclusions that the knowledge database doesn't strictly support, but instead merely implies or hints at.

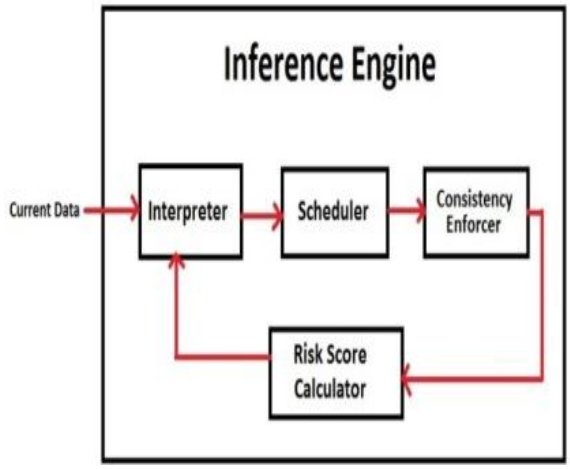

Fig 3.2:Inference Engine

The inference engine is the program part of an expert system. It represents a problem solving model which uses the rules in the knowledge base and the situation-specific knowledge in the working memory to solve a problem.

1. Interpreter: The interpreter executes the chosen agenda items by applying the corresponding base rules.
2. A scheduler. The scheduler maintains control over the agenda by estimating the effects of applying inference rules in light of item priorities or other criteria on the agenda.
3. A consistency enforcer. The consistency enforcer attempts to maintain a consistent representation of the emerging solution.

   Explanation System: Expert systems typically need to be able to provide explanations regarding the conclusions they make. Most expert systems provide a mechanism whereby the user can ask questions about:

- why a particular question is being asked
- how the system came to a particular conclusion

  Providing explanations is essential in all non-trivial domains for the user to understand how the system works and determine whether its reasoning is correct or not. Typically the system will keep track of what rules (knowledge) it is using and provide explanations based on a translation of these rules into English.

IV. RISK SCORE CALCULATION

The heart and soul of the process of identification of abnormalities in users' behaviour lies in the module of risk score calculation. The calculation of the risk score is based on the following risk components.

- IP addressof the user's device (i):

The user's IP address will serve to categorize users according to their location. For the purpose of calculating the risk value of this component, IP threat values have been assigned to various countries of the world. A higher value indicates a greater risk value. Values have been assigned taking into consideration the extent of terrorism existent in those countries. Figure 5.2 shows the assigned values.

- User's current location (Loc):

During the process of checkout, an additional field called 'Current Location' has been provided in order to further validate the user. A mismatch in the location entered by the user and the location denoted by the recorded IP address would serve to identify an illegal user.

- The time at which a user logs in (L_t):

Frequent users generally adhere to specific periods of logging into a site. Any deviation from this pattern will serve to increase the user's the risk value for this component as well as enable the system to absorb this change in user behaviour and incorporate it into the knowledgebase as new knowledge.

- Time difference between login and logout (T_d):

Carefully observed trends state that the occurrence of a considerable time span between a legal user's login and logout activity. However, if this time span turns out to be less that the predetermined limit (assumed as 3 minutes for our system) then this change in behaviour will reflect an increase in the risk value of that particular user

Using the above mention risk components or factors, the risk score of a particular user activity will be calculated as follows

$$R_s = \frac{\sum Rc}{L}$$

Where,Rs = Risk Score
Rc = score associated with the Risk Component.
L = Risk Limit set by an individual E-business firm.
Usr = username
Psw = password
L_t= Login Time
Loc= Location
T_d=Time difference between login and logout

Ip	Usr	Psw	Loc	L_t	T_d
170.132.1.116	abc1	%#$	4	3	4
170.132.1.116	abc1	%#$	4	4	6
170.132.1.116	abc1	%#$	4	4	4
109.205.115.0	abc1	%#$	8	5	6

Fig 4.1:Knowledge Base Data

Figure 5.1 is a representation of a sample of data collected in the knowledgebase which pertains to a specific user whose username is 'abc' and password in an encrypted form is '%#$'. The first three rows are indications of a legal user whereas the last row is a clear indication of an illegal user who has gained access to the account by unfair means. A graph of legal user behaviour V/S illegal user behaviour has been shown in figure 4.3

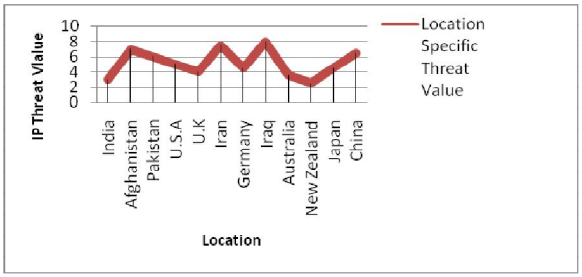

Fig4.2:Location specific threat value

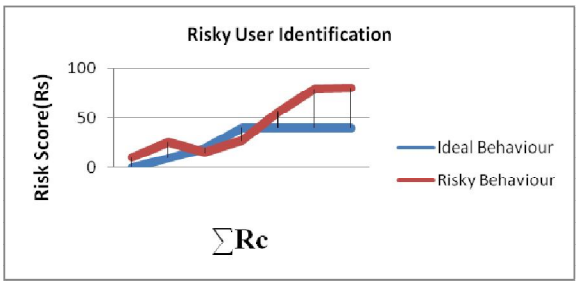

Fig4.3:Behaviour of different users

The process of risk score calculation is intended to work continuously in the background while the user performs certain activities on the foreground. Shift in customary user behaviour will be easily identified by the risk score since each behavioural shift will lead to a rise in the risk score. If the increased value of the risk score is well within the predetermined risk limit, the expert system assumes this to deviation in behaviour to be a new user attribute and therefore, engages itself in a self-learning and reasoning process. However, if the risk score exceeds the predetermined limit, the expert system will identify this to be major threat to the sanctity of the user's transaction and thus will either terminate the current transaction or provide challenges to the current user for authentication. A terminated activity will then open for investigation by whosoever it may concern. The explanation system of the expert system will help to provide backtracking to the cause of the termination thereby leading to the identification of the source of malicious online activity.

V. SYSTEMARCHITECTURE

The above diagram shows the overall system architecture. This system architecture includes the following components.

- E-commerce portal
- Structured Database
- Inference Engine
- Domain Specific Knowledge Base
- Explanation System

The E-commerce transaction process starts when a registered user logs into an e-commerce website. The inference engine then correlates the registered user's data with the data in the knowledge base and based on risk score of that user, allows the user to proceed for further transaction. But if the user is not a registered user, then the registration form will appear which when filled will get updated in the knowledge base after Normalization.

So, whenever a registered user logs in, all his data and previous transaction will be correlated in the inference engine. This inference engine will then calculate the risk-score using the risk score calculator with the help of specified parameters. If this risk score is within the pre-defined limit, the user is allowed for further transaction. Else it will stop that particular user's transaction and lead to further investigation.

Typically the system will keep track of what rules (knowledge) it is using and provide explanations based on a translation of these rules.

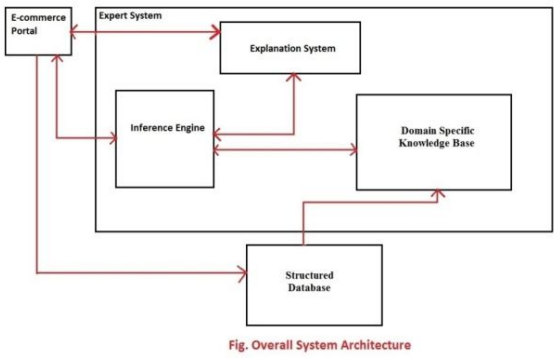

Fig 5.1:Overall system architecture

CONCLUSION AND FUTURE SCOPE:

Enhancement of the security of E-commerce is the need of the hour. The growing industry brings with it a promise of profits in millions of dollars at the same time; inefficient security mechanisms against the abstract nature of cyber-attacks can bring an E-

commerce firm a grave loss of millions of dollars as well. In order to maximize the profits and minimize the danger of potential losses, the development of a permanent security solution is a must. This paper introduces the concept of the inclusion of an expert system for permanently enhancing the security of E-commerce. Inclusion of additional parameters other than the aforementioned ones for the purpose of risk score calculation can be incorporated into the system with considerable flexibility.Through the detailed information provided in the paper, deployment of such a mechanism for enhancing security on other domains would prove to be extremely beneficial. Also, the scope and boundaries of the applications of the proposed system advantageously extend far into the unforeseeable future.

REFERENCES:

[1] Pablo. How people shop online – Ecommerce Statistics. [Cited:Aug27, 2012]. [http://www.fortune3.com/blog/2012/08/how-people-shop-online-ecommerce-statistics/]

[2] Wikipedia. E-commerce. [http://en.wikipedia.org/wiki/E-commerce]

[3] E-commerce: Lack of consumer trust holds it back [http://www.ipsos-mori.com/researchpublications/ researcharchive/ 1603/ECommerce-Lack-Of-Consumer-Trust-Holds-It-Back.aspx]

[4] Dave Chaffey. E-business and E-commerce management. Pearson publication, 3rd edition, 2009, ISBN 978-81-317-2518-4

[5] Introduction to E-commerce. Sage publications[www.sagepub.in/upm-data/9598_019964Ch1.pdf]

[6] The Psychology of Security,By Bruce Schneier ,January 18, 2008, [https://www.schneier.com/essay-155.html]

[7] Fostering Consumer trust and purchase intention in B2C e-commerce, by Siddhi Pittayachawan, [http://www.academia.edu/1858056/Fostering_consumer_trust_and_purchase_intention_in_B2C_e-commerce]

[8] Strategies for the security of online payments in e-commerce, by Chen Zhang, Shijie Jiang, Bin Huang, ICCIA 2012.

[9] Architecture of expert system, By JokoPurwadi

[10] Major components of Expert system,[year12ipt.ash.com/untitled-7.html]

[11] What is an inference engine, [www.wisegreek.com/what-is-an-inference-engine.htm]

[12] An effective knowledge base architecture and issues in representation techniques, by PoonamTanwar, Dr. T. V. Prasad, Dr.KamleshDatta.

[13] Expert Systems: An Introduction, by K S R Anjaneyulu.

★★★