Smart Mode of Tackling E-Commerce Security Cyber Crimes through Biometric Face Identification Technique Applying Holistic Approach

T. Kalaichelvi, PhD
Professor,
Department of CSE,
Panimalar Institute of Technology, Chennai-600123

S. Hemalatha, PhD
Professor,
Department of CSE,
Panimalar Institute of Technology, Chennai-600123

P. Aishwarya
Student, Second year,
Department of CSE,
Panimalar Institute of Technology, Chennai-600123

S. Aiswarya
Student, Second Year,
Department of CSE,
Panimalar Institute of Technology, Chennai-600123

ABSTRACT

The security systems used currently does not provide required levels of safety against towering threats. The prominent reason for their failure is the usage of point solutions for protecting hosts and reactive approach against intrusions. Electronic Commerce is process of doing business through networking. A person sitting can access all the facilities of the Internet to buy or sell the products from the place he is stationed. Security is the challenge faced by e-commerce today & there is still a lot of advancements to be made in security features. The one aspect where e-commerce wins over traditional commerce is that the buyer can browse online shops, compare and order merchandise on their PC. The researches imply the significance of the e-commerce in developing countries for business concerns.

Keywords

Intrusion detection system, managerial security controls, operational security controls, technical security controls,Face Recognition, Holistic Matching Methods, Feature-based (structural) Methods, Hybrid Methods

1. INTRODUCTION

Electronic commerce is a term used to signify any type of trade or transaction, that requires the transfer of data across the Internet. It covers an array of different types of businesses, from consumer based market sites, through auction sites, to market exchanges trading goods and services. It is currently one of the most trending aspects of the Internet to emerge.

1.1 Working of E-Commerce

The consumer surfs the internet to reach the merchant's web site. Then, he decides what he wants to purchase , whereafter he is moved to the online transaction server, where all his information given is encrypted. Once the order has been placed , the information moves through a private gateway to a Processing Network, where the issuing and acquiring banks complete or deny the transaction. This generally takes place within 5-7seconds.

For improving the use of e-commerce in developing countries it is implemented for increasing access to global markets for enterprises situated in developing countries. For a developing country advancement in the field of e-commerce is the need of the hour.

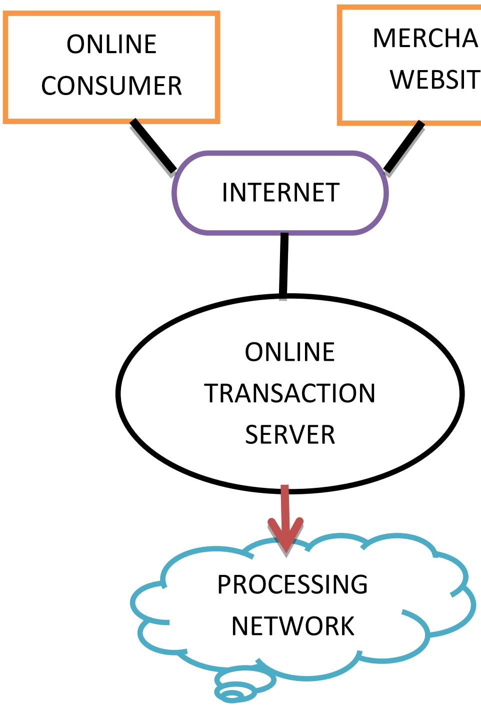


Fig.1.1 : Working of E-Commerce

2. RELATED WORK

This paper[1] has presented network security system that is based on application of features from immunity of human system to enhance security of the systems. The system has embedded features which assist information security system to adapt to changing environments. Secure mobile agents which are produced and tested using negative and clonal selection algorithms, are used to protect systems and networks. The secure mobile agents that satisfy the specifications are allowed to perform the intrusion detection, vulnerability analysis, security management services and intrusion response. The paper incorporates the system using secure mobile agents whose inputs come from sensors like Firewall, SNORT, Osiris and Nessus. Mobile agents process the feed from sensors and based on specifications of the subsystem perform different activities and in the end, the result is given using sensors.

The next paper[2] states that despite the popular image of the hacker breaking into a computer system from the outside, most computer intrusions are committed from within the organization by employees. This paper states that misuse intrusion architecture of information system (IS) security effectiveness that stops, finds, supervises and redeems employee fraud. IS security effectiveness as far as this architecture is concerned refers to the ability of IS security steps to defend against unauthorized misuse of IS assets by users. Improper use of IS includes tampering of software, impairment of hardware, embezzlement of data,abuse of Internet and unauthorized use or intentional interruption of computer services. This architecture is designed effectively to safeguard organization's data as it follows a holistic approach that includes all aspects of security to combat employee problems.

The main aim of the author in[4], was to put forth a extensible design for Intrusion Prevention System.An overall idea of the IPS has been given where the combination of a number of security solutions has been investgated. The paper focuses on the Intrusion Response, Intrusion Detection and Post Vulnerability Analysis and Elimination.

A Distributed Denial of Service attack[5] is a main stream coordinated attack on the availability of services of a victim system, indirectly launched via compromised computers. Intrusion detection systems are network security tools which process local audit data and also check network traffic to analyze for required patterns or obvious deviations from expected behavior.The study states dis-tributed intrusion detection methods to detect Distributed Denial of Service attacks in a training set and test these methods in simulated-real time environment, in which the mobile agents are synchronized with the timestamp of modification.Each of the stated method involves the usage of signals generated by SNORT, a signature-based network intrusion detection system. The qualification criteria of the methods is based on network load, reliability, and mean detection time values.

Th paper[6] is based on vulnerability scanners (VSs),which are nothing but information security tools which can detect security weaknesses on hosts in a network. VSs secure hosts in a dedicated way. An ardent approach is prefered to be better than reactive approaches followed by, for example, intrusion detection systems. There are many technical glitches and disadvantages of currently available VSs, such as tarnishing system resources while conducting scans. This paper introduces a conceptual model for vulnerability forecasting. The model makes use of innovative techniques to improve on the efficiency of currently available VSs. The model fixes its goal at its ability to do vulnerability forecasting especially by predicting the finite number of known vulnerabilities which may come by using intelligent techniques and vulnerability history of the data. A prototype is used to test the model and the results are also provided in the paper.

3. EXISTING SYSTEM

When traditional commerce is compared with e-commerce there are many glitches which needs to be taken care of. The major problem is the limited ability of the buyer to interact with the product. The next big problem that e-commerce has been facing recently is that of its security. Traditional buyers and sellers are still apprehensive about conducting business online. The buyers of US comprising of 70% people are genuinely concerned about the security of online transactions. This factor dampens the enthusiasm of consumers from using credit cards to shop online.

3.1 Some recent technological breakthroughs:

Verifi, DigiScent's iSmell and TouchSense are the technologies that have been developed in the last few years in order to enhance online shopping experience. Even though iSmell and TouchSense are very new technologies and also most of the sellers haven't implemented them, they promise a consumer-friendly future. Verifi is one technology that has been extensively adopted.

3.2 The Reality of E-Marketplaces

3.2.1.Direct Buyer/Seller Links: Allows sellers to post direct links from a web site to the websites of their own company. Interested buyers can click these links to a vendor's web site. Or else,there maybe no link and only direct contact information about particular firm is present

3.2.2. Line auctions On: Applications may take three forms

1. Listing-agent auctions: Here the service provider acts as an agent who runs web-based auctions on the concern of private sellers who list their own auctions.
2. Merchant auctions:Here no private sellers are identified, and the service provider acts as a marketing agent, which conduct its transactions by auction.

3.2.3Request for quots: Here the seller or buyer informs that he has a desire to sell or buy products. Buyers and sellers may be unable to select the firms to which their quotes . Messages may include price information.

3.2.4.Trade Leads/Classifies: Here the seller or buyer informs that he has a desire to sell or buy products.The interested people have complete control over which user forms can access messages posted to the forum. Messages generally do not include price information.

3.2.5.E-Retail: The service provider sells products directly to users. Visitors take the role of buyers and the site provider takes the role of a seller.

3.3 Technical Hitch

- There can be lack of system security, reliability due to improper implementation of e-Commerce.
- Software development industry is one of the industries that keeps getting updated every day.
- Network bandwidth might cause an issue as there is insufficient telecommunication in some countries due to lack of available bandwidth.
- E-commerce environment may demand specific types of software required for vendor setting apart from network servers.
- Integrating E-Commerce software or website with the existing application or databases is difficult at times.
- E-Commerce software may be incompatible with some operating system or any other component which can cause an compatability issue.

3.4 Non-Technical Disadvantages

- Initial cost: The cost of building E-Commerce application in-house is very high. Hence there could be delay in launching the E-Commerce application due to lack of experience.
- User resistance: User cannot believe the site being unknown seller. Hence,such things makes it difficult for the user switch from physical stores to online/virtual stores.
- Security/ Privacy: Very tedious to ensure security or privacy on online transaction process.
- The touch or feel of products during online shopping is very low.
- E-Commerce applications are still evolving and changing rapidly.
- The access of internet is still not cheaper but it is inconvenient to use for many potential customers who reside in remote villages.

4. SYSTEM OVERVIEW

The goal of this thesis is to propose an approach which not only can detect both known and unknown attacks, but can also actively prevent from occurring, which is done by introducing the Intrusion Prevention System (IPS). Another goal was, to propose a simple and flexible distribute

d IPS architecture that eliminates the inherent shortcomings (like static nature, vulnerability to direct attacks, scalability, etc.) found in the earlier IDSs architectures. For the realization of Thesis Goal an effective Intrusion Prevention System based on Mobile Agents will be proposed.

One of the most tangible solutions for the threats that are faced by e-commerce retailers will be**" FACE RECOGNITION TECHNIQUE"**.The basic principle of the face recognition technique is comparing the image that is already present in the database with the current image that is taken during the transaction period.

This involves extracts its features and then recognize it, regardless of lighting, expression, decoration, the process of growing old, transformations (translate, rotate and scale image) and pose, which is a difficult task..

The first section describes the common methods namely holistic matching method, feature extraction method and hybrid methods. The second section describes applications with examples and finally third section describes the future research directions of face recognition.

Biometric-based techniques have emerged as the most promising option for recognizing individuals in recent years since, instead of certifying people and allowing them access to physical and effective domains based on passwords, PINs, smart cards, tokens, keys and so, these methods examine an individual's physiological and behavioral characteristics in order to find and discover his/her identity.

Passwords and PINs are very difficult to remember and which can be easily stolen or guessed;Similarly cards, tokens, keys and the like can be incorrectly positioned, forgotten, or duplicated; magnetic cards can become corrupted and unclear.

4.1 Face Recognition Methods

Face recognition is such a challenging yet interesting problem that it has attracted researchers who have different views and backgrounds.

The following methods are used to face recognition:

1. Holistic Matching Methods
2. Feature-based (structural) Methods
3. Hybrid Methods

4.1.1. Holistic Matching Methods:

In holistic approach, the complete face region is taken into account as input data into face catching system

(1) The first stage is to insert a set of images into a database, these images are names as the training set and this is because they might be taken into account when we compare images and when we create the eigenfaces.

(2) The second stage is to discover the eigenfaces. Eigenfaces are made by taking the characteristic features from the faces.

The input images are brought to line up the eyes and mouths. They are then resized to its original size.

Eigenfaces can now be extracted from the image data by using a calculating tool called Principal Component Analysis (PCA).

(3) The eigenfaces have been created such that each image will be represented as a vector of weights.

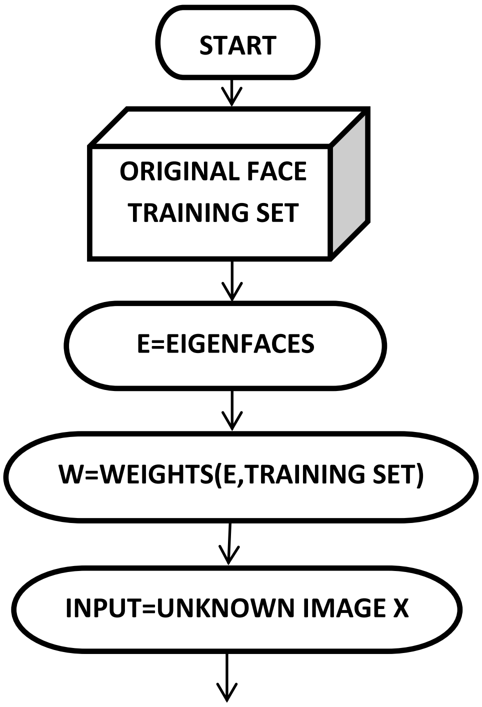
(4) The system is now ready such that it can accept entering questions.

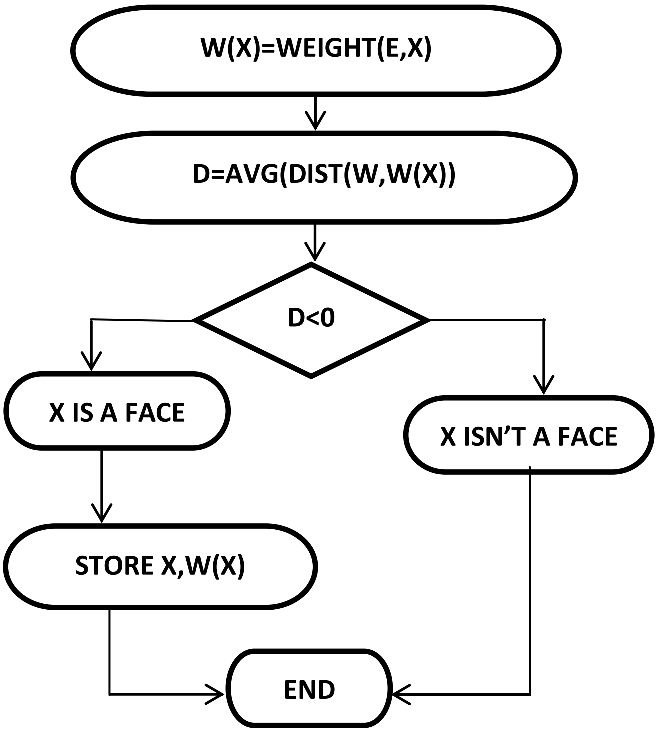
(5) The weight of the unknown incoming image is found and then compared to the weights of those present already in the system.

(6).If the input image's weight is above a given threshold value,then it is considered to be not recognised.

The identification of the input image is performed by detecting the image in the database whose weights are almost the closest to the weights of the given input image.

(7). The image in the database with the closest weight will be returned as a hit to the user of the system.





4.1.1: Flow chart for Holistic matching method

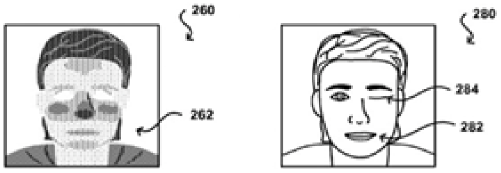
4.1.2. Feature-based (structural) Methods:

In this methods biological features such as eyes, nose and mouth are first of all extracted and their positions and local statistics (geometric and appearance) are fed into a structural classifier. A big challenge for feature extraction methods is feature "restoration", this is when the system tries to retrieve features that are invisible due to large variations, e.g. Pose of the head when we are matching' a frontal picture with a profile picture. It distinguishes between three different extraction methods:

I. Generic methods based on edges, lines, and curves
II. Feature-template-based methods
III. Structural matching methods that includes geometrical Constraints on the features.

4.1.3.Hybrid Methods:

A combination of both holistic and feature extraction methods is nothing but Hybrid face recognition systems . Generally 3D Images are used in hybrid methods. The image of a person's face is caught in 3D, allowing the system to note down the curves of the eye sockets, for example, or the shapes of the forehead or chin . Even a face in profile would serve because the system uses depth, and an axis of ordinates, which gives it enough information to construct a whole face. The 3D system usually proceeds thus: finding, Position, Measurement, portrayal and Matching.



5. COMPARISON OF TECHNIQUES

This section gives the detail about the results of the experiments described above .Search space is too big to be generated explicitly; since we aim for a conservative estimate that approximates by excess the capabilities of the attacker, we implemented the algorithm so that it would always return a guess that is something worth less of the search space size. Those experiments with this approximated technique results in a relative error of the order of 5%.

5.1 Based on Password Strength:

In the figure given below, the fraction of passwords guessed is plotted as a function of the search space size in our three datasets. Everytime, the results are similar qualitatively. With k values getting higher k, better results are obtained for the weaker passwords because of the more precise modeling retrieved here. However, the passwords that include k graphs not represented in the training set cannot be guessed. Methods dealing with smaller k values become effective as they generalize . Practically, the most effective strategy will be to weigh it based on the resources of the intruder, measured in terms of number of attempts. Dictionary attacks and mangling techniques produce better guesses when the search space has a size.

The effect of diminishing returns is felt here also, while selecting the optimal value of k for each case, considering the IT dataset, around 100,000 attempts need to be tried in order to guess 20% of the passwords (k= 5). This figure increases to roughly 1.1 billion candidates to guess 40% of the passwords (k= 3). Also the search space needed to break 90% of the passwords increases to approximately 3.

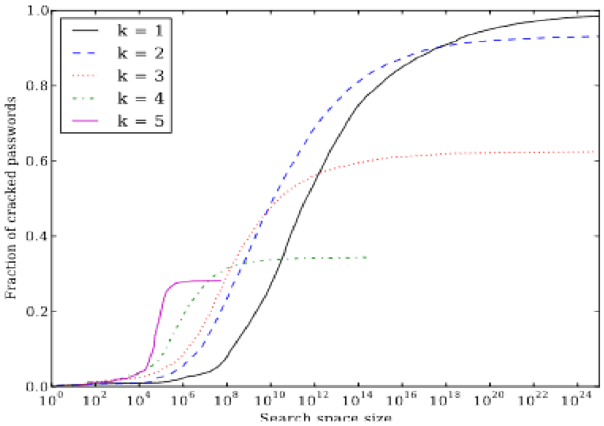


Fig 5.1: Comparison Based On Password Strength

Why are biometrics secure?

- Unique: The various biometrics systems have been developed from unique characteristics of each and every individual. The probability of 2 people sharing the identical biometric data is virtually nil.
- Cannot be shared: Because a biometric property is an innate property of every individual, it is extremely tedious to make copies of the same or share.
- Cannot be copied: Biometric characteristics are nearly impossible to forge or imitate, especially with new emerging technologies ensuring that the biometric being identified is from a live person.
- Cannot be lost: A biometric property of an individual can be lost only if a serious accident occurs

6. CONCLUSION

A whole new variety of techniques has been developed to find people since the 1960s from the measurement and exmination of parts of their bodies to DNA profiles. Forms of identification are used to ensure that every citizens are desirable for rights to benefits and to vote without fear of impression while private individuals have used seals and signatures for centuries to lay claim to the existing and personal estate. Generally, the amount of proof of identity that is essential to gain access to something is proportionate to the value of what is being learnt. It is found out that only 4% of online transactions use methods other than simple passwords. Security of systems resources generally follows a three-step process of identification, authentication and authorization. Today, a high level of belief is as deprecatory to E-Commerce transactions as it is to conventional face-to-face transactions.Thus it is commonly trusted that face recognition technique will prove to be the best solution for E-Commerce problems and issues.

7. REFERENCES

[1] MagicNET: The Human Immune System and Network Security System ,Muhammad Awais Shibli, Jeffy Mwakalinga,, and Sead Muftic, Department of Computer and System Science DSV, The Royal Institute of Technology (KTH), Stockholm Sweden, SU/KTH, DSV, Borgarfjordsgatan 15, SE-164 40 Kista, Sweden, NUST School of Electrical Engineering and Computer Sciences, Islamabad, Pakistan

[2] N.T. Baloyi. Misuse intrusion architecture: prevent, detect, monitor and recover employee fraud, The Proceedings of the Information Security South Africa 2005 New knowledge today conference. Sandtorn, South Africa.

[3] Twycross, J.P. Integrated innate and adaptive artificial immune systems applied to process anomaly detectionUniversity of Nottingham. 2007.

[4] S. Ahmed, S. Muftic, Intrusion Prevention System based on Secure Mobile Agents , Thesis Report, Department of Computer and Systems Sciences (DSV-KTH), March 2006.

[5] P. Kannadiga, M. Zulkernine, DIDMA: A Distributed Intrusion Detection System Using Mobile Agents , Proceedings of the Sixth International Conference on SE. Vol , Issue , 23-25 May 2005

[6] Vulnerability Forecasting – conceptual Model" by H.S. Venter and J.H.P. Eloff, Computer & Security (2004) ELSEVIER

[7] Cyber Security Risks Assessment with Bayesian Defense Graphs and Architectural modelsTeodor, Sommestad Royal Institute of Technology teodors@ics.kth.se Mathias Ekstedt, Royal Institute of Technology mek101@ics.kth.se Pontus Johnson,Royal Institute of Technology ,pj101@ics.kth.s

[8] Shibli, M. A., & Muftic, S. (Feburary 2009). MagicNET: Security Architecture for Creation, classification and validation of Trusted Mobile Agents

[9] Jung Won Kim, Integrating artificial Immune Algorithms for Intrusion Detection, Ph. D thesis, The Department of Computer Science, University of London, 2002

[10] Jung Won K.; Bentley, P, The Human Immune System and Network Intrusion Detection, Department of Computer Science, University of London, Gower Street, London, WCIE 6BT, U.K