

PRIVACY PRESERVING AND USER IDENTITY TRACKING SYSTEM AT CYBER CAFE

K.Dhivya¹, Prof.T.JebaMoses.M.Tech²

¹(Information Technology, IFET College Of Engineering, Villupuram, India, dhivyask@gmail.com)

²(Faculty-Information Technology, IFET College Of Engineering, Villupuram, India, jebamosesmtech@gmail.com)

Abstract—Now-a- days the Cyber bistro's plays an essential part in Internet. Any illegal activities happen in and around the urban areas. The digital bistro in charge don't have any detail about the user who enter into the digital bistro . To keep away from these issues to the legislature needs to take an activity to control the digital bistro as concentrated one. This application makes all the digital bistro to gather in less than one tree. Utilizing this application all bistro can be added to the database and the administrator of that bistro is given by an id and password. Utilizing that id and password the subtle elements of the bistro can be kept up by the administrator like framework information and client data. To track a client details are stored in database with an id verification. After enlistment of the client the admin is given by an id . This id is broadly remarkable. Since it is an exceptional id the clients ID can be checked broadly in any digital caf s. So the clients need not to convey the id proofs while they go for caf .

Keywords—Cyber cafe; User Identity; User Validation

1. INTRODUCTION

Data security dangers obliterate the estimation of e-business. The proprietors of Internet bistros amplify the flexibility of utilization of Internet access to the group yet they neglect to fix their PC security to defend the private data of their clients. The point of this study is to give data to enhancing data security in the Internet Cafe deliberately to guarantee information protection, information trustworthiness, hazard administration and security consistence. The study examines the data security issues that are confronted by clients of Internet bistros and investigates the impacts of these issues. It demonstrates how clients can enhance their physical security to reach higher measures of data protection over the Internet. Much research has been led on the subject of data security yet this exploration introduced here concentrates for the most part on the issues that face clients of Internet bistros and the change of open PC securities to protect clients' data from programmers and malware. The study concentrates on Internet bistros and clients situated in India.

In Lucknow, India District Administration makes a new order all over India. The order says, "Cyber cafe owners will allow only those to surf the net who produce a reliable identity proof like voter identity card, ration card, driving licence, passport, etc. In case they fail to produce a proof of their identity, they should not be allowed the service." [1] Notably, the order is one of the five points which have been finalized in wake of the recent spurt in terrorist activities. The order issued by district magistrate Chandra Bhanu said that stern action will be initiated under section 188 of the Indian Penal Code (IPC) in case a cyber cafe owner violated the said norms. The same order said that the cyber cafe owners will have to maintain a log book wherein the details of every customer will be maintained. The log book must carry the sub heads of name, address, telephone number and the identity proof produced by the individual.

The owners must also ensure that the person who has come to use the cyber cafe fills the log book in his own hand writing. A minimum record of at least six months will have to

be maintained by the owners. For example: If a person opened the log book on August 1, 2015, then he has to keep it till January 31, 2016.

2. RELATED WORKS

Information security threats destroy the value of e-business. The owners of Internet caf s extend the freedom of use of Internet access to the community but they fail to tighten their computer security to safeguard the private information of their customers. The aim of this study is to provide information for improving information security in the Internet Cafe strategically to ensure data privacy, data integrity, risk management and security compliance. The study investigates the information security issues that are faced by users of Internet caf s and explores the effects of these issues. It shows how users can improve their physical security to reach higher standards of information privacy over the Internet [2].

Much research has been conducted on the subject of information security but this research presented here focuses mainly on the issues that face users of Internet caf s and the improvement of public computer securities to safeguard users' information from hackers and malware. The study focuses on Internet cafes and users located in India.

The studies found that majority of users are affected by information security issues such as viruses, scam, online harassment, information privacy and many more. The study also found that the users were also responsible to those issues due to their behaviour towards information security technologies such as antivirus software, password and physical security. User where not using strong password, they were forgetting to logout from their accounts, some were working on computers that the antivirus software was turned off.

Users of Internet caf s face serious challenges when it comes to information security in Internet caf s. The Internet caf  owners usually fail to cover all angles of information security, and in this way they breach the trust of their customers. Although they increase the freedom of customers

to use the Internet, they don't improve their computer security to protect customer information from hackers and malicious damage.

Digital security is the movement of ensuring data and data frameworks (systems, PCs, information bases, server farms and applications) with fitting procedural and mechanical efforts to establish safety. Firewalls, antivirus programming, and other mechanical answers for shielding individual information and PC systems are key yet not adequate to guarantee security. As our country quickly constructing its Cyber-Infrastructure, it is similarly imperative that we instruct our populace to work appropriately with this framework. Digital Ethics, Cyber-Safety, and Cyber-Security issues should be coordinated in the instructive procedure starting at an early age. Security counter measures guarantee the classification, accessibility, and trustworthiness of data frameworks by keeping or relieving resource misfortunes from Cyber security assaults. As of late digital security has developed as a built up order for PC frameworks and infrastructures with an attention on insurance of significant data put away on those frameworks from adversaries who need to get, degenerate, harm, devastate or deny access to it. An Intrusion Detection System (IDS) is a project that investigations what happens or has happened amid an execution and tries to discover signs that the PC has been abused. An extensive variety of analogies was considered, including those identifying with: military and different sorts of contention, natural, human services, markets, three-dimensional space, and physical resource assurance. These thus prompted thought of an assortment of conceivable methodologies for enhancing digital security later on. These methodologies were marked "Heterogeneity", "Motivating Secure Behavior" and "Digital Wellness"[3].

Digital Security assumes an essential part in the advancement of data innovation and also Internet administrations. Our consideration is normally drawn on "Digital Security" when we find out about "Digital Crimes". Our first thought on "National Cyber Security" in this way begins on how great is our base for taking care of "Digital Crimes". This paper concentrate on digital security developing patterns while embracing new advancements, for example, portable registering, distributed computing, e-business, and long range informal communication. The paper additionally depicts the difficulties because of absence of coordination between Security offices and the Critical IT Infrastructure.

3. PROPOSED SYSTEM

Nowadays the Cyber café's plays a vital role in Internet. It may take place in and around the cities. But it does not have any identification. The people who enter into the cyber café also don't have any identity. So it takes lot of drawbacks in maintaining the details of the peoples who enters the café for browsing. To avoid these problems to the government has to take an initiative to control the cyber café as centralized one.

This application helps to make all the cyber café to group in under one tree. Using this application a new café can be added to the database and the admin of that café is provided

by an id and password. Using that id and password the details of the café can be maintained by the admin like system info and user info. To track an user the details are stored in database with an id proof. After registration the user is provided by an id and password. This id is nationally unique. Since it is a unique id the user's identification can be verified nationally in any cyber café's. So the user needs not to carry the id proofs while they go for cafe's.

4. OBJECTIVES

To monitor the cyber café with the details provided by the user. The user can verify the information from the existing users' identity. The detail entered by the user is found to be false then the admin of the café incharge does not allow them to browse. This thesis is used to maintain the user information of the browsing candidates. The details given by the customer is verified from the list of identities. If the user is coming for the first time for browsing he/she has to give the details of his information. The details or identity given by them is verified by the list of identity. The admin can add new cabin. The browsing and printing history is stored in the database for future use.

5. ADVANTAGE

- The users' accurate information is added in the database.
- The user need not to carry the identity proofs everywhere
- The details given by the user is verified by the café in charge.
- The café details and accounts are maintained in the database for future use.

6. SYSTEM ARCHITECTURE

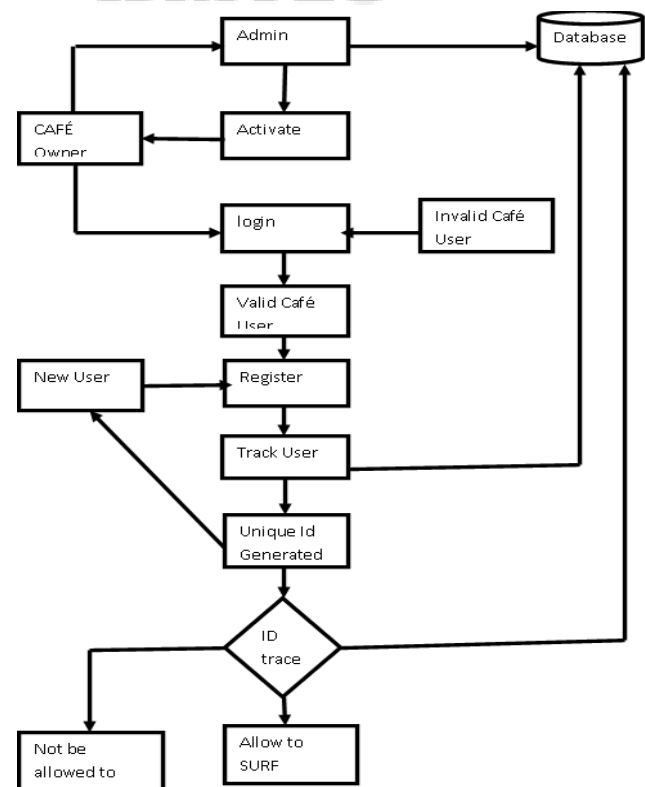


Fig 1 System Architecture

7. CONCLUSION

Using this project the admin can track a single user identity while they are in café. So that they can't give fake entry such as name, address, mobile no, email id, etc. Their identity are verified by the information given by the authority. After completion the problems in the existing system would overcome. The "Cyber Café Monitoring And Administration System" process made computerized to reduce human errors and to increase the efficiency. The maintenance of the records is made efficient, as all the records are stored in the SQL Server database, through which data can be retrieved easily. The application has been tested with sample data and it is found to be working in a perfect manner. This system has been developed as a user friendly and easy to operate. This system has been developed in such a way that any changes can be made easily in future if necessary. The new system promise to be accurate, adequate and time saving need of the concern.

REFERENCES

- [1] <http://timesofindia.indiatimes.com/city/lucknow/ID-proof-must-for-cyber-cafe-users/articleshow/3358736.cms>
- [2] Information Security Issues Facing Internet Café Users, Alfred Thaga Kgopa, 2013
- [3] Cyber security: challenges for society- literature review Atul M. Tonge, Suraj S. Kasture , Surbhi R. Chaudhari, 2013
- [4] D. J. Bodeau, R. Graubart, and J. Fabius-Greene, —Improving cyber security and mission assurance via cyber preparedness (Cyber Prep) Levels, September 9, 2010.
- [5] Audry Watters, Read Write Cloud, RWW Solution Series, 2010
- [6] Amichai Shulan, Application Defence Center (ADC), Amicha Regularly Lectures, Security, 2011
- [7] Bibliothequesolvay, parLeopold, Security and Defense Agenda, 137 rue Belliard, B-1040 Brussels, Belgium
- [8] Ajith Abraham¹, Crina Grosan², Yuehui Chen³, Cyber Security and the Evolution of Intrusion Detection Systems, School of Computer Science and Engineering, Chung-Ang University, Korea ²Department of Computer Science Babes-Bolyai University, Cluj-Napoca, 3400, Romania ³School of Information Science and Engineering Jinan University, Jinan 250022, P.R.China
- [9] Denning D., An Intrusion-Detection Model, IEEE Transactions on Software Engineering, Vol. SE-13, No. 2, pp.222-232, 1987.
- [10] Ravi Sharma, Study of Latest Emerging Trends on Cyber Security and its challenges to Society, International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1 ISSN 2229-5518 IJSER © 2012
- [11] Abraham D. Sofaer, David Clark, Whitfield Diffie, Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy <http://www.nap.edu/catalog/12997.html> Cyber Security and International Agreements ,Internet Corporation for Assigned Names and Numbers pg185-205
- [12] [ThillaRajaretnam Associate Lecturer, School of Law, University of Western Sydney, The Society of Digital Information and Wireless Communications (SDIWC),International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 232-240 2012 (ISSN: 2305-0012)