Third International Conference on "Materials, Computing and Communication Technologies"
in association with International Journal of Scientific Research in Science,
Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

Improving The Security of Internet Banking System Using Three Level Security Implementation

(Smt) K. Amutha MCA M.Phil.[1], V. Deivanai[2]

[1]Assistant Professor, Department of Computer Science, Sri Sarada College for Women (Autonomous), Tirunelveli, Tamil Nadu, India

[2]II MSc Computer Science, Department of Computer Science, Sri Sarada College for Women (Autonomous), Tirunelveli, Tamil Nadu, India

ABSTRACT

Bank server is an innovative technology that can be used for processing and sharing data in a safe manner. Data may be processed and shared securely across an inconsistent network using a bank server, This project proposes with a brief history of the security system and explain some of the most important aspects of this new technology. When it comes to identify the potentially harmful transactions on an untrusted network, machine learning may be an effective tool for deciphering massive datasets. Using these clever strategies in conjunction with each other is critical in banking and finance. The public Elliptic dataset from many banks is utilized as a baseline for our proposal, which is then implemented to Secure this system. SHA Secure Hash Algorithm is used as a trustworthy gateway to the internet banking since the latter is not completely labeled. The data is then classified using four machine learning approaches. When CNN Convolutional Neural Network and random forest classifier are combined, the suggested method displays promising results

Indexed terms: Machine Learning, Secure Hash Algorithm, Convolutional Neural Network, Principal Component Analysis (PCN).

I. INTRODUCTION

Online banking is now the subject of a great deal of study, and a large number of financial institutions provide their services over the internet. However, there are some limitations to this method, such as the fact that if a family has many members, visiting various websites and memorizing numerous login passwords is necessary in order to get information about each member's transactions and accounts. A single login ID and password is all that is required for the customer to access the integrated system in this suggested solution. It is possible for the user to conduct many bank transactions with a single identification number[1]. The system administrator and the bank administrator are the other two users of this suggested system.

New banks and branches may be added by system administrators who can also see information on branch managers and approve or reject registrations for these institutions. They may register themselves and if the

bank's administrator approves, they can access information about their branch clients' accounts. Cyber-attacks on Internet banking systems are increasing in number, complexity, and pervasiveness at an accelerating rate. This raises the issue of whether the online business model is sustainable. There is a lack of effort to address the vulnerabilities connected with the client's soft-components (PC, Internet browser, and End User) in most Banks' current security systems, which instead focus on offering a distinct method for remotely verifying transaction data.[6]. Using a PC infected with financial malware and a non-hardened Internet browser to conduct financial transactions is a risk that cannot be ignored, according to this paper's findings. Because there are so many active endpoint attack vectors, cybercriminals may create sophisticated assaults that affect the behavior of the End User, resulting to either canceled or fraudulent transactions. End users who are the victims of cyber crime are not only financially harmed, but their privacy and security may be affected for a long time after the fraud is done and perhaps compensated. This is contrary to what most people believe. As a result of this study, it is possible to increase Internet banking security and efficiency by incorporating both hardware and software components into the transaction system, but yet maintain user convenience and privacy. As it turns out, a PC-connected piece of hardware is necessary for providing tamper-proof storage and a safe environment for hardened software programs to run on. It is hoped that by providing End Users with a workable solution, the hackers' work would be made much more difficult, cutting their profit margins and helping to restore a more even playing field in the war against cybercrime.

II. EXISTING SYSTEM

The existing online banking system has its own user interface and database which maintains all the records of its customers and branch managers. For accessing different bank accounts, the user has to visit multiple bank websites which enquires the user to remember multiple login credentials. It may not be easy for all the users to remember all the login ids and passwords. Also, the current banking system has certain limitations such as the transactions can be made only between certain timings and sometimes the user is not provided the access to many functions in the application[3]. The existing work on security for Internet Banking talks about a model that solves most of the security related problems encountered in internet banking systems.

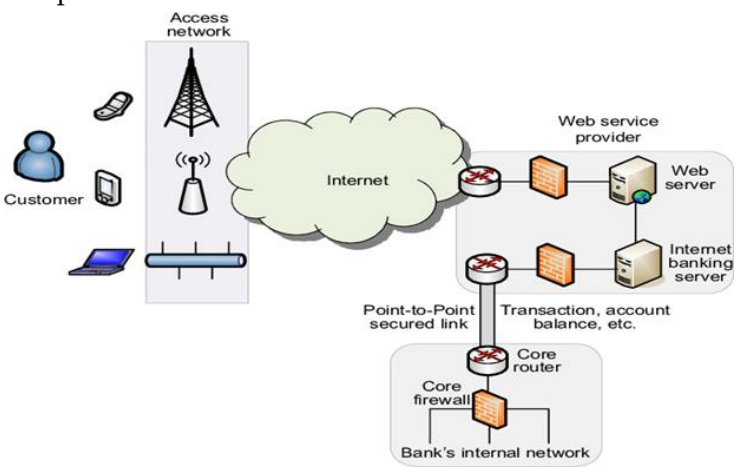
- Digital Certificates: Digital certificates are used to authenticate both the users and the banking system itself. This kind of authentication depends on the existence of a Public Key Infrastructure (PKI) and a Certificate Authority (CA), which represents a trusted third-party who signs the certificates attesting their validity.
- One-Time Password Tokens: One-Time Password devices are used as a second authentication factor. This kind of devices render captured authentication data useless for future attacks through the use of dynamically changing passwords which can be used only once.
- Browser Protection: In this model, the system is secured at the Internet browser level, which is used to access the banking system. The user and their browser are protected against known malware by monitoring the memory area allocated by the browser in order to detect such malware and hinder credential theft and capturing of sensitive information.

- CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans is a method adopted to render automated attacks against authenticated session effective. This method requires the legitimate user to input information conveyed as scrambled images which are difficult for automated robots to process and recognize.
- Transaction Monitoring: This is currently applied in all online banking systems, using different techniques. Artificial intelligence, transaction history analysis, intrusion detection system, intrusion prevention system and other methods that identify fraud patterns in previously processed transactions are among the various approaches used. But there are certain issues with above mentioned implementations.

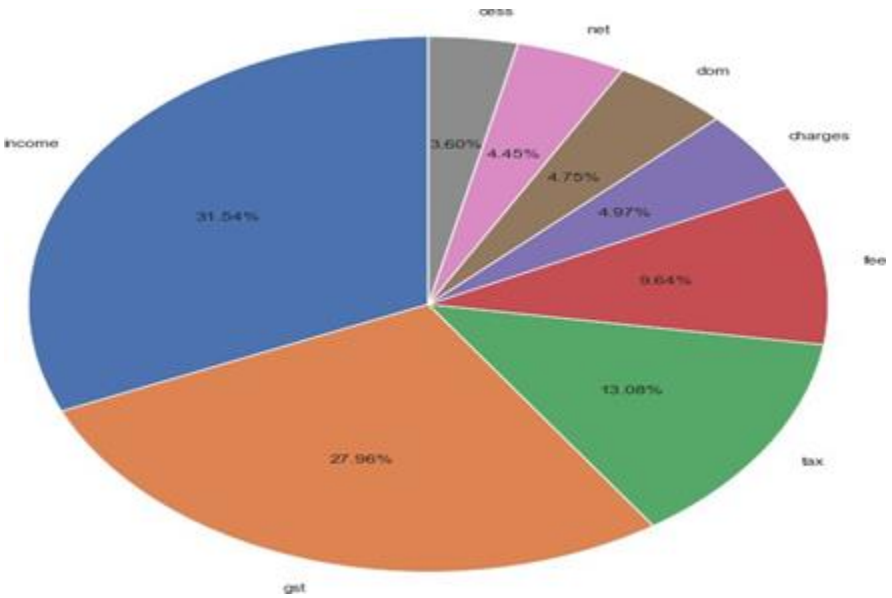
III. PROPOSED SYSTEM

Online banking provides countless advantages for both banking industry and its users. It enables the customers to make huge transactions worth several millions or simple transactions worth few rupees in matter of seconds without visiting the bank physically. Thus, customers have no need to wait in long queues to retrieve bank services. Online banking is ease of access and time serving[2]. From banks perspective, saving can be made from reducing staff remuneration, branch office, and Automatic Teller Machine (ATM) and Electronic Funds Transfer at Point of Sale (EFTPOS) transaction maintenance budgets.[10] Providing banking services with the necessary security from a remote location through the internet is a challenging process in banking sector. Probability of attacks increase with the advancement of online banking services. Billions of financial data transaction is conducted online every day. Thus not achieving a perception of security will have the wider effect of reducing customers' trust in internet banking as well as the bank. Skilled criminal hackers' carryout bank cyber-crime attacks everyday by manipulating the banks' online information system. Ensuring perfect security in online banking is hard to achieve target with rational client.[5]-[6].

Emerging new Technologies and large-scale businesses have made this world, a global village. Many business organizations provide online services targeting global consumer bases. Transaction in international scale has been enabled by banks all around the world through E-banking in order to supply the needs of above business organizations[5]. E-banking serves lots of benefits to both customers of banks and banks itself. It adds value to customer's satisfaction with better service quality and enables banks to gain a competitive advantage over other competitors



IV. RESULT



In this diagram Data analyzation of gst, tax, income charges are shown in percentage mode to accomplished in priority order.

V. CONCLUSION

As the crave for a more secure Internet banking system and service continues to rise, there is no doubt that the development and deployment of the system proposed in this work will go a long way in solving our Internet banking security needs. The system proposed here will guarantee a trusted path to the customer rather than trusting the customers computers. This will eliminate any possible occurrence of the "Man in the Middle" attacks or other attacks which have been recurrent. This proposed system will not only solve our security needs, but will also make Internet banking affordable to the majority of the world population, guaranteeing security of customers' accounts and information. The Internet enhances the interaction between two businesses as well as between individuals and businesses[9]. As a result of the growth of the Internet, electronic commerce has emerged and offered tremendous market potential for today's businesses. One industry that benefits from this new communication channel is the banking industry.

VI.REFERENCES

[1]. W. Henecka, S. K Ögl, A.-R. Sadeghi, T. Schneider, and I. Wehrenberg, "TASTY: Tool for automating secure two-party computations," in Proc.17th ACM Conf. Comput. Commun. Secur. (CCS), 2010, pp. 451–462.

[2]. R. Bost, R. A. Popa, S. Tu, and S. Goldwasser, "Machine learning classification over encrypted data," in Proc. Netw. Distrib. Syst. Secur. Symp.,2015, p. 4325.

[3]. R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in Proc. 53rd Annu. Allerton Conf. Commun., Control, Comput. (Allerton),Sep. 2015, pp. 1310–1321.

[4]. R. Gilad-Bachrach, N. Dowlin, K. Laine, K. Lauter, M. Naehrig, and J. Wernsing, "Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy," in Proc. Int. Conf. Mach. Learn.,2016, pp. 201–210.

[5]. A. Nordrum, "Popular Internet of Things forecast of 50 billion devices by2020 is outdated," IEEE Spectr., vol. 18, Aug. 2016.

[6]. X. Liu, R. Deng, K.-K.-R. Choo, and Y. Yang, "Privacy-preserving outsourced clinical decision support system in the cloud," IEEE Trans. Services Comput., early access, Nov. 15, 2017, doi: 10.1109/TSC.2017.2773604.

[7]. T. Feng, D. J. Wu, M. Naehrig, and K. Lauter, "Secure computer evaluationof k-nearest neighbor models," U.S. Patent 9 825 758, Nov. 21, 2017.

[8]. D. Reinsel, J. Gantz, and J. Rydning, "Data age 2025: The evolution ofdata to life-critical," Don't Focus Big Data, pp. 2–24, Apr. 2017.

[9]. H. Park, P. Kim, H. Kim, K.-W. Park, and Y. Lee, "Efficient machine learning over encrypted data with non-interactive communication," Comput.Standards Interfaces, vol. 58, pp. 87–108, May 2018.

[10].X. Liu, R. H. Deng, K.-K.-R. Choo, and Y. Yang, "Privacy-preserving outsourced support vector machine design for secure drug discovery,"IEEE Trans. Cloud Comput., vol. 8, no. 2, pp. 610–622, Apr. 2020.