Anomaly Based Detection and Prevention of Phishing Attack in An Online Banking System

Prof. C. S. Pagar[1] , Nihal Rajpurohit[2], Devendra Patil[2], Manish Ganeshkar[2]

[1]Assistant Professor, Information Technology, SKNSITS, Lonavala, Maharashtra, India

[2]U.G. Student, Information Technology, SKNSITS, Lonavala, Maharashtra, India

ABSTRACT

Now days online banking and electronic payment gateways are the trending factor. Day by day more technologies invented to hack accounts as well bank servers. Phishing is one type of attack in which attacker gain access to users account using respective stolen credentials. Many commercial products are there for providing banking cloud security (CS) for these online banking activities. But no such noble tool or system till date invented to prevent phishing attacks. These types of attacks increased now days. Internet banking is mostly used by everyone. Generally, each bank has got its own service of contract with respect to internet banking. Due to this the online banking application have become more challenging.

In our system we developed anomaly-based detection. It decreases the chances of getting account hacked through a phishing technique. In advance we have to provide additional security with the help of IP detection and device detection.

Keywords: Cloud Security, Internet Banking, Internet Protocol, Anomaly Based Detection

I. INTRODUCTION

Online banking has become a most reliable trend now-a-days and security related to the same is becoming a challenge to us. Authentication using passwords is vulnerable to attacks like phishing; thus we have to invent the system known anomaly based detection and prevention of phishing attacks. Providing security to a customer's financial information is vital and therefore banks and other financial institutes offer different security mechanisms to reduce the risk of unauthorized access to their online customer accounts. Most of the attacks on online banking systems are based on deceiving the user to reveal their login details and then the attacker will use those stolen credentials to gain unauthorized access to the customer accounts. Phishing attacks and social engineering methods are mostly used to deceive the online account users. As most of the phishing attacks are targeting the financial sector, protecting online banking systems from phishing attacks is a major concern. Failing to provide a proper security assurance will reduce the growth and damage the reputation of online banking services. Even though there are several researches already being carried out and commercial products are available to secure online banking systems, they have their own ups and downs.

II. LITERATURE SURVEY

Surbhi Gupta et al., [1] examines about the Phishing social building assault hypothetically and their issues in the life of human beings. Phishing is regularly completed by Email caricaturing or texting. It focuses on the client who has no learning about social building assaults, and web security, similar to people who don't deal with protection of their records points of interest, for example, Facebook, Gmail, credit banks accounts and other money related records. The paper talks about different sorts of Phishing assaults, for example, Tab-resting, parodying messages, Trojan steed, hacking and how to avert them. In the meantime this paper additionally gives diverse procedures to distinguish these assaults so they can be effortlessly managed in the event that one of them happens. The paper gives an intensive investigation of different Phishing assaults alongside their focal advantages and disadvantages.

SANS Institute et al, [2] presented an inside and out examination of phishing: what it is, the innovations and security shortcomings it exploits, the risks it stances to end clients, and bits of knowledge into what should be possible to check the impacts of this wrongdoing. In this investigation I will clarify the ideas and innovation behind phishing, indicate how the risk is significantly more than only a disturbance or passing pattern, and examine how groups of lawbreakers are utilizing these tricks to make a lot of cash. I will give a few insights and proposals you can use to shield yourself from these tricks utilizing barrier inside and out procedures, and clarify a maybe a couple of the devices and advances being produced to battle the genuine danger of wholesale fraud what's more, online misrepresentation.

Ibrahim Waziri et al, [3] exhibits that attempt to identify the different types of website forgery phishing attacks and non-technical countermeasure that could be used by users, (mostly by non IT users) that lack the understanding of how phishing attack works and how they can prevent themselves from these criminals. In this technological era, everyone connects to the internet either using a computer or some sort of a mobile device. Financial transactions, academic registrations etc. are mostly conducted online. Later in this paper we will characterize what phishing assault is, the means by which phishers actualize phishing assaults and how clients can separate between a real site and a pernicious one.

Guardian Analytics et al,[4] finds that anomaly detection solutions are promptly accessible, are sent rapidly (particularly SaaS arrangements), and instantly and consequently ensure all record holders against a wide range of misrepresentation assault with negligible disturbance to genuine web based keeping money movement. Executing peculiarity discovery won't just meet. Business and retail account holders at money related establishments of all sizes are under assault by refined, sorted out, very much supported digital lawbreakers. These assaults have brought about billions of dollars lost and harmed connections between monetary foundations and their record holders.

LongfeiWu et al, [5] examines report on the security vulnerabilities caused by portable phishing assaults, including the web page phishing assaults, the application phishing assaults, and the account library phishing assaults. Existing plans outlined for web phishing assaults on PCs can't adequately address the different phishing attacks on cell phones. Henceforth, we propose MobiFish, a novel computerized lightweight enemy of phishing plan for versatile stages.

Patrick Lacharme et al, [6] has been finds user authentication is typically based on two or more factors.

Nevertheless, the development of various malwares and social engineering attacks transform the user’s PC in an untrusted device and thereby making user authentication vulnerable. This paper investigates how user authentication with biometrics can be made more robust in the online banking context by using a specific device called Off PAD. This context requires that authentication is realized by the bank and not only by the user (or by the personal device) contrary to standard banking systems.

Markus Goldstein1 et al, [7] investigates anomaly detection is the process of identifying unexpected items or events in datasets, which differ from the norm. In contrast to standard classification tasks, anomaly detection is often applied on unlabelled data, taking only the internal structure of the dataset into account. This challenge is known as unsupervised anomaly detection and is addressed in many practical applications.

S. Manasa et al. [8] has been introduced that phishing is an online criminal activity using the collection of social engineering methods such as messages and emails to make the users to disclose their sensitive information such as personal details, username /password4, etc. Since 2007 Net-Banking transactions are the target of the phishers. The strong techniques are required to avoid phishing attacks. In our paper, we proposed Multi Factor Authentication (MFA) and secure session key generation using Gaussian distribution to reduce the attacks caused by the phishers.

Priyanka Mahajan1et al. [9] has been studied that the banking and financial systems have been totally changed due to the environment and globalization changes and competition of business services . Internet Banking or Web Banking or Online banking is used to describe banking transactions through internet application. Online Banking means user can get connected to his bank's website by using his personal computer system and web browser. But there are many security problems like fraudulent websites, fake emails from banks, capturing user IDs and passwords, hacking personal bank accounts and steal money etc.

Abhida Shende et al. [10] has been examined that biometric recognition systems are nowadays playing important role in authentication field. The physiological features like Fingerprint and hand geometry, Iris, DNA, Palm print, Retina, face, Ear, etc. are used to differentiate between individuals. Among these iris is unique organ which can be used for secured authentication and avoids unauthorized access.

III. METHODOLOGY USED IN PROPOSED SYSTEM

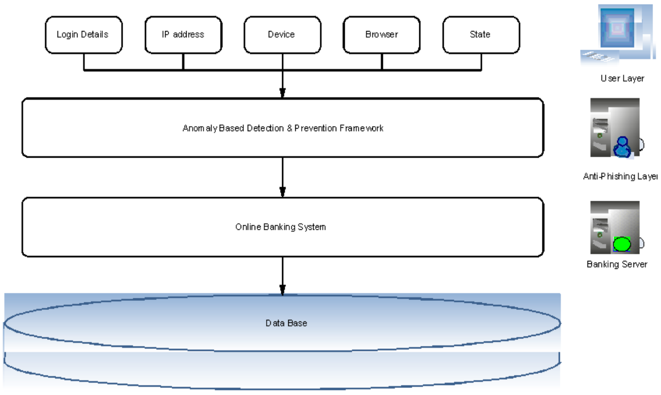


Figure 1. System Architecture

Step1:- When Costumer first time login to System that time all details IP address, current device, OS, time, location stored user log files at bank server for future anomaly detection.

Step2:- Next time when user want to login that time these details compared with users current details if matched then access granted otherwise security Questions asked to user if ok with this then n only then access granted.

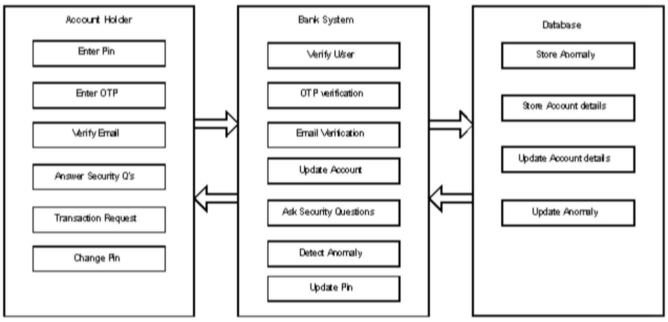


Figure 2. Block Diagram

All security steps completed then all 3 mechanisms applied to verify user is valid or not.

A. Anomaly Based detection:-

It is the process of detection of unusual or suspected behaviour of user or a system. If user or system

detected suspected that time anomaly breaks so user gives another chance to prove its authenticated user by asking Security Questions and Mail Confirmation as well as OTP confirmation.
eg. Spam Asian provides Bayesian mechanism for email spam detection.

B. IP Address Based Detection:-

User try to access via Foreign IP(Out of range IP) instead Local IP(range is predefined) that time user will confirmed via a mail.

C. Device Based Detection:-

If user trying to access with new device that time also security check needed .Security Questions asked plus OTP confirmation applied. Every user should be register his device as a default device means cookies stored in his device and should be update cookies for security. Above all three steps fails then 3 chance given to user for proving his identity if yes then ok else blocked account

IV. RESULTS AND DISCUSSION

Table 1. Results

Security	Primary Action	Secondary Action	Access
IP Detection	Set IP	Check IP	No
OS Detection	Set OS	Check OS	No
Browser	Default Browser	Check Browser	No
Device Detection	Default Device	Check Device	No
Security Token	Set Token	Get Token	Yes

In Our proposed work we worked on the challenges already faced by existing system. To overcome the drawbacks in existing work we have to implement the anomaly based detection and prevention of phishing attacks. In this first of all we need to some additional information from users at time of account opening or new registration of account through an online banking system. At time of account opening we have to get information such as user details, IP address of user's system, device of user (make it default), browser of user, user base location etc. After that this all information should be stored in user log files of banks servers and also stored in users default devices in the form of cookies. When next time user or any other person should try to access the information that time previously stored anomalies matched then and only then users get access to its account. There is rare chance that the person who is trying to access the account is authenticated user. But some kind of issue he can't use his own device or his location as well IP changed. That time our anomaly based detection system give chance to user that he prove his identity by using mobile OTP confirmation as well as mail verification. In advance the security question should be faced and should be giving the correct answers otherwise user's account gets blocked. User should go to respective bank to activate it again.

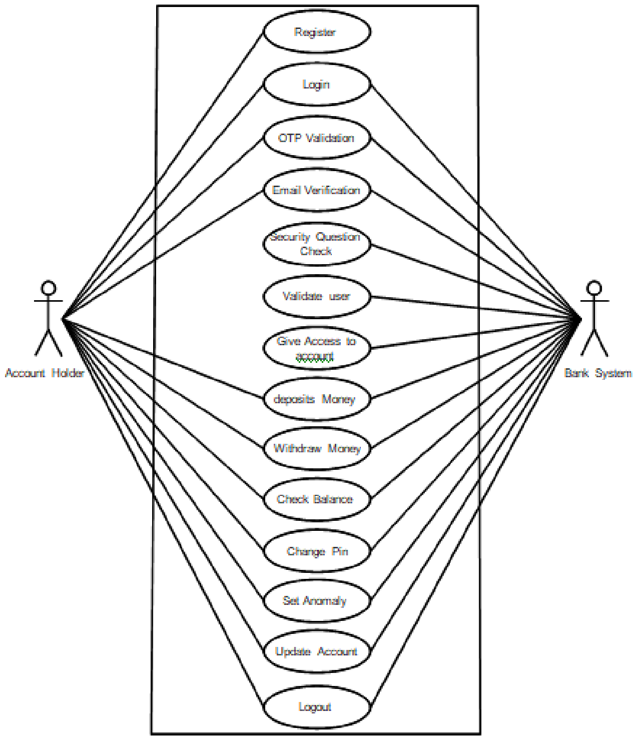


Figure 3. Activity Of System

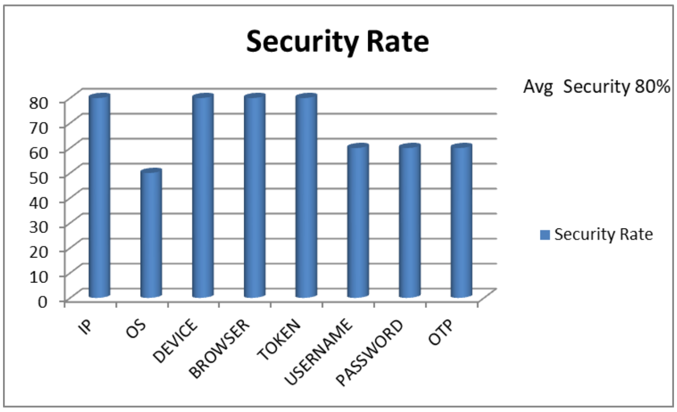
1. User Module:

- User login to the system, after login user gets authentication permission to access or view system.
- At a time of login user details get stored in user log files and this log file stored in banks server.
- User current location, browser, Operating system, device, IP address stored as a anomalies. .
- User has to set security question at first time login.

2. System Module:

- System gets logged in after that user having already successfully registered.
- System is responsible for giving access to user by simply matching anomalies if matched then ok otherwise check for identity.
- First of all OTP get verified then email confirmation gets verified after that security question gets asked to user.
- All these steps get successfully verified by respective users then get access to user otherwise user gets blocked.
- If user gets blocked then user needs to go to respective bank to reopen the account.

Security Rate Graph



Graph 1. Increased Security Rate

Advantages:

- The objective of the proposed system is to provide high security to user's account as well as users credentials.
- Although credentials get stolen but user gets surety that account get secured by anomaly framework.
- We are recommendation of anomaly based detection schema for gets better security and reliability.
- Security in our system is very high as compared with existing schema.
- This is proved that our system get differentiate actual user and attacker even though both having same username and password.

V. CONCLUSION

Thus we implemented the anomaly based detection and prevention frame work to accurately detect phishing attacks before they happened. We reduced the harm of these attacks as much as possible. The overall system will not only detect the unauthorized login attempts but also prevent it, notified to authorized users and safeguard online banking customers from fraudsters.

In future we have to implement the multi factor authentication with the reduction of verification steps by taking advantage of anomaly based detection. We would try to detect and prevent unauthorized login attempts by biometric multifactor authentication.

VI. REFERENCES

[1]. Surbhi Gupta et al., 'A Literature Survey on Social Engineering Attacks: Phishing Attack," in International Conference on Computing, Communication and Automation (ICCCA2016), ISBN:978-1-5090-1666-2/2016, pp. 537-540.

[2]. SANS Institute, "Phishing: An Analysis of a Growing Problem",online] Available from: https://www.sans.org/readingroom/whitepapers/threats/phishing-analysis-growing-problem-1417 January 2007.

[3]. Ibrahim Waziri Jr, "Website Forgery: Understanding Phishing Attacks & Nontechnical Countermeasures," in IEEE 2nd International Conference on Cyber Security and Cloud Computing, pp. 445-450, 2015.

[4]. Guardian Analytics, "A Practical Guide to Anomaly Detection Implications of meeting new FFIEC minimum expectations for layered security", Online] Available from: https://www.aba.com/Tools/Offers/Documents/GuardianPracticalGuidetoAnomalyDetection.pdf, May 2011.

[5]. LongfeiWu et al..,"Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms," in IEEE Transactions On Vehicular Technology, DOI 10.1109/TVT.2015.2472993, 12 April 2016, pp. 6678-6691)

[6]. Patrick Lacharme st al, "One-Time Biometrics for Online Banking and Electronic Payment Authentication" , Research gate . Sept 2014.

[7]. Markus Goldstein1 et al, "A Comparative Evaluation of Unsupervised Anomaly Detection Algorithms for Multivariate Data" , PLOS ONE | DOI:10.1371/journal.pone.0152173 April 19, 2016

[8]. S. Manasa et al. , "Securing Online Bank Transactions from Phishing Attacks using MFA and Secure Session Key" , Indian Journal of Science and Technology, Vol 8(S2), 123–126, January 2015

[9]. Priyanka Mahajan1 et al, "Secured Internet Banking Using Fingerprint Authentication" IJIRCCE DOI: 10.15680/IJIRCCE.2016. 0403271.

[10]. AbhidaShende et al, "Enhancing the Security of Internet Banking using Iris Biometrics"