ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

A Survey on Anomaly Based Detection and Prevention of Phishing Attack in an Online Banking System

Manish Ganeshkar[1], Devendra Patil[1], Nihal Rajpurohit[1] , Chetan Pagar[2]

UG Student, Information Technology, SKN SITS, Pune, India[1]

Assistant Professor, Information Technology, SKN SITS, Pune, India[2]

ABSTRACT: Now day's 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 user's 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 applications 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

1. A Literature Survey on Social Engineering Attacks: Phishing Attack

The paper 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

DOI: 10.15680/IJIRCCE.2018. 0611004

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.

2. Phishing: An Analysis of a Growing Problem

This paper gives 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.

3. Website Forgery: Understanding Phishing Attacks & Nontechnical Countermeasures

In this paper we 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.

4. A Practical Guide to Anomaly Detection Implications of meeting new FFIEC minimum expectations for layered security

This paper presents, 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.

5. Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms

In this paper we completed a thorough 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.

III.EXISTING SYSTEM APPROACH

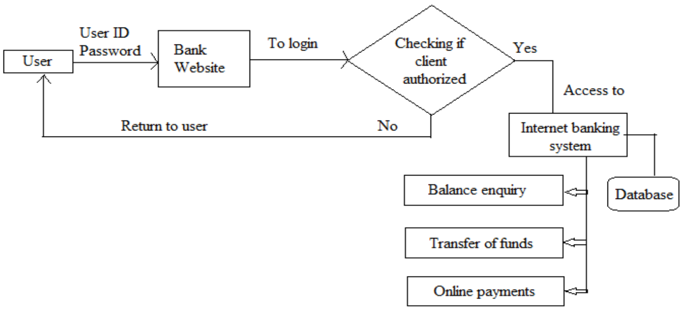

Fig.1 Block Diagram of Existing System

In existing system some techniques used to prevent the attacks on bank accounts and bank servers. Among this methods unable to detect the phishing type attack because attacker get logged in to a system by using users credentials which may not be detected easily that this user is authenticated or not. In existing banking security frameworks design by considering server side security. In this system tells to users keeping your password private & change it regularly. Password combination make it strong so should not be easily break. Antivirus should be installed and updated in our personal computers. Should not give reply to fraud links and spam mails. Don’t disclose your account information to anyone.

But these entire things not enough to prevent and detect phishing type attacks. So there is need of some advanced technique should be detect the phishing attacks before they happen and take some actions accordingly.

IV.PROPOSED SYSTEM APPROACH

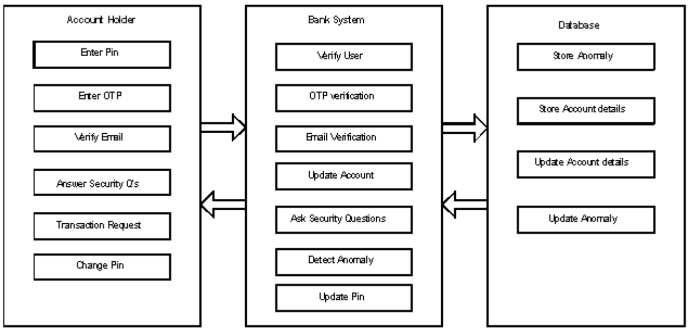

Fig.2 Block Diagram of Proposed System

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.

V.SYSTEM ARCHITECTURE

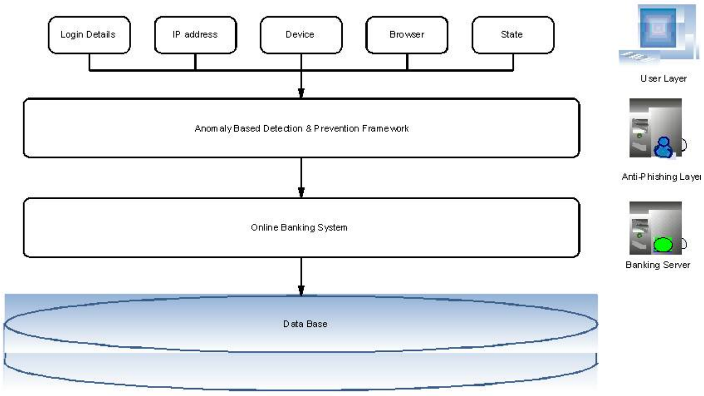

Fig.3 System Architecture

METHODOLOGY USED IN PROPOSED SYSTEM:

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.

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 Adreess 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.

VI. CONCLUTION

In proposed work we have used the anomaly based detection and prevention of phishing attacks before they happened. We reduced the harm of these attacks as much as possible. There are some limitations to this system like every time location, IP and device detection makes users more inconvenience to use the online banking system.

VII. Future Work

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.

VIII. Acknowledgment

This work is supported in a Anti-phishing online banking system of any state in India. Authors are thankful to Faculty of Engineering and Technology (FET), Savitribai Phule Pune University, Pune for providing the facility to carry out the research work.

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.

BIOGRAPHY

First Author – Manish Ganeshkar, B.E, SKNSITS
Second Author – Devendra Patil, B.E, SKNSITS
Third Author – Nihal Rajpurohit, B.E, SKNSITS
Correspondence Author – Chetan Pagar, B.E, SKNSITS