Smart Intelligent Computing and Communication Technology
V.D. Ambeth Kumar et al. (Eds.)

doi:10.3233/APC210044

A Review Based on Secure Banking Application Against Server Attacks

Revathy P[a,1] and Belshia Jebamalar G[b]
[a]*Associate Professor, Dept of CSE, Rajalakshmi Engineering College, Chennai, India*
[b]*PG Student, Dept of CSE, Rajalakshmi Engineering College, Chennai, India*

Abstract. In recent years, attacks on online based transaction become very common and are widespread, which makes the banking server compromised by using users account and personal informationwithout authorization. To address the security concerns, also gain user trust and confidentiality, we propose automatic detecting and prevent bank attacks such as DDOS and SQL injection. Also, to eliminate bot-based attacks we enhance security at the authentication phase by invoking OTPthereby preventing brute force attack. The proposed system generates unique CAPTCHA for validating the user transaction. Hence it is difficult for intruder to perform unauthorized activities within the banking application. Finally,the proposed system secures user password from traditional approach using negative password generation technique. Thus, we conclude by combining all the three techniques together for the secured bankingapplication.

Keywords. Distributed Denial of Service, SQL injection, Brute force attack and Negative password generation

1. Introduction

Cyber security plays an important role in financial sector. Mainly in banking since foundation of banking lies in trust, confidentiality and credibility. Its important role is to protect our sensitive and personal data. It also defends the entire network from the malicious customer assets. Nowadays especially during the covid times, more people go with cashless transaction so many fraudulent activities are done through online, as a result customer loses the trust in banks and other financial institutions here cyber security deals and resolves to give solution this problem by protection their data. This paper has taken two major attacks like DDOS and SQL injection. Denial of service means the attackers carefully craft the traffic to overload a firewall in an effective manner. Another method of overloading is that making all virtual machinessends dummy packets with no payload to the target firewall as the background traffic. Distributed Denial of Service (DDOS) is an attack which threatened the target system.

[1]Revathy P,Associate Professor, Dept of CSE, Rajalakshmi Engineering College, Chennai, India;
E-mail: -revathy@gmail.com

It includes traffic like sending messages, fake packets and incoming calls by sending to server and network which they can't take control. Main purpose of this is to stop the legitimate user in utilizing the website. Sometimes it has tendency to divert the destination. When we focus on the target the cybercriminal takes this time to cheat us by installing malicious software or by stealing the data. This attack is mainly done on the servers and makes the transactions impossible. In this system we are trying to provide solution to all the attacks.SQL Injection (SQLi) is an attack which allows the attacker to inject the malicious query and possibly try all the ways to execute it. This has an ability to retrieve all the data from SQL database in order to exploit the customer personal and sensitive data. Database includes customer personal information, property details, trade secrets, transaction details and so on. if these details reach the fraud hands he can modify, insert, delete and anything might happen so this is considered to be most dangerous vulnerabilities of the banking application. It is really hard to prevent these vulnerabilities. The process actually begins with web page input and slowly reaches the query now the attacker starts to inject all malicious code which then automatically executed. It can even attack the network which is located behind.We also enhance our security to prevent brute force attack. Mostly recent days brute force attack is done by bots so that has become bot-based attack. The process involves in predicting our passwords by number of trials. Trials include guessing and also fetch the combination to reach the actual passwords. This attack is an oldest attack but still it exists. The process involves cracking which mainly depends on the length and complexity. Sometimes our antivirus protects us from this attack if it is not available then our system is at higher risk. Once the password has been cracked then automatically all our personal data will reach the hackers hand which can result a great loss for the customer in the banking application. The objective of the project is to style and develop a secure application for banking which detects intrusion and prevent the application from all these attacks by providing solution which invokes CAPTCHA along with OTP generation added to that the new method called encrypted negative password generation technique has been introduced. Completely Automated Public Turing Test (CAPTCHA) is actually detects whether the user is human being or not. Bots are generally used for brute force attacks if the CAPTCHA is given the bot can't able to identify all those letters so bot may not be allowed to log in further. One Time Password (OTP) is a static password which can be used only once and can't be reused. It is used to authenticate which generates a unique numeric code for each and every transaction. Timing is always synchronized with these OTP in order to make the transaction safe and secured. OTP changes every 30 or 60 seconds, depending on how the time is configured with tokens. It is very common in online banking and purchase. Since OTP is unique it is extremely difficult for the hackers to predict it. This are send to the user phone through SMS or by push messages. OTP tokens are of software based and are difficult to predict or keep track by the hardware. Encrypted Negative Password technique (ENP) is a newly introduced password preserving technique. It receives the plain password from the user which is hashed via cryptographic hash function that is SHA 256. The obtained hashed password is converted into negative password which is again encrypted into the encrypted negative password using symmetric key algorithm (AES). This method is extremely difficult for the hacker to crack the password as a result they have a lot of complication to reach our sensitive data. This technique eliminates data breaches in the traditional existing approach. In this all these three techniques are merged in the single application. For experimental results, banking-based web application is developed using Java frameworks to integrate the proposed.

2. Related Works

Nancy Nainan,SumaiyaThaseen and HimikaParmar (2012)proposed an authentication service that is based on image and of time synchronized OTP which helps the system to identify the legitimate user. The OTP is unique and can change after the regular interval but can't be utilized after the stipulated time. Venkata Krishna Reddy,G. SowmyaandD.Jamuna (2012) proposed a system which prevents brute force attack by blocking method. This paper ensures high security where hacker find difficulty in assessing the user accounts.

VidehPaliwal, B. C. Julme, SukrutBadhe, Vikrant Bhise and NinadNarayane (2014)Proposed and explained SQL injection attack patterns and prevention algorithm against the SQL Injection Attack. This includes scheme namely static and dynamic phase. phase maintains anomaly pattern and all queries are checked in the static side. Alarm will indicate the new form of anomaly and those patterns will be generated in dynamic side.

AnandPandey (2015) developed a combined schema which gives the idea to maintain the password for any system along with alphanumeric type. This makes user simple and they have no necessary to memorize the difficult passwords.

Chithra (2013) presented many available algorithms which have been used to prevent the internet services from the DDOS attack. Also describes the strength and weakness all the available algorithm. This helps to understand problem in better way and also help in analyzing the right algorithm to particular problem on DDOStreat. Dave, KonarkTruptiben (2015) provide solution to the attacks. Here brute force attack is generally meant that hacker guesses the combination of numbers and letters to crack the actual one. Many people have tendency to forget and some are lazy so might use simple passwords and utilize the same for all. These people are highly at risk so this paper gives solution to that problem by defending against the hackers.Pooja, Monika (2016) proposed the techniques which actually detects andprovide methods for preventing SQL injection. This includes malicious code which has been injected in the database. In this paper for prevention approach called negative tainting is used along with two modules. This paper will detect the malicious code before the execution. This paper also discusses about the types of SQL injections and their strength along with its weakness. Upendra Singh, SurabhiAgrawal (2017) introduced botnet which frequently launch the Distributed Denial-of-Service (DDOS) overwhelm which hides an "army" of compromised nodes in the network. The application layer can lead to the number of possibilities to conceal the malicious activities exploited by the botnet which is performed by the emergence of attacks. RudreshGurav, Leena Dabhade, AbhilashKulkarni, Amar Agarwal, Rahul Chinchore (2018) introduced Coverage to deal with the relation between the personal data and password. Probabilistic Context-Free Grammars (PCFG) guesses and try to crack the password based on the information used. This attack in common bothin online and in offline mode.S.Soundharya, K.RaviKumar (2018) described that Internet is broadly used in every viable field in the modern times. In this busy world the data in the database and also in the public can be attacked through various techniques. One of the techniques to attack the database is SQL Injection attack which involves the unauthorized access to the SQL queries and cause damage to the execution also steal all the data which are kept personally. This paper uses PHP for attacks and storing all data in the database and Java is considered as the host language.WenjianLuo (2019) proposed an ENP

technique with higher security. Encrypted Negative Password technique (ENP) is a newly introduced password preserving technique. It receives the plain password from the user which is hashed via SHA 256 which is again encrypted via symmetric key algorithm. This method extremely difficult for the hacker to crack the password as a result they have a lot of complication to reach our sensitive data.SachinJadhav, Sana Jamadar, PoojaLande, Gayatri Mane (2019) proposed a secret word verification system. This system contains two phases namely registration and authentication phase. Instead of password they receive secret word from the client and apply hash function which then encrypted to encrypted negative password by utilizing the symmetric key calculation and multi emphasis encryption.Nice Mathew and Salwa P.B (2019) utilized the RSA algorithm for the final encryption in order to secure password. . It receives the plain password from the user again the encryption process is carried via the RSA algorithm for more protection.
PradeepKumar,Poornima,Subathra S, andNivetha (2020) proposed the authentication technique despite of many security laws. The proposed system has high secure password storage where the plain password is hashed. Now obtained password is converted to negative later the negative form to encrypted negative password (ENP).it is extremely difficult for to crack the ENP. This resists the lookup table attack and protects the dictionaryattack.BibinVarghese, JittyMerinMathewandSmita C Thomas (2020) proposed the k-hidden algorithm since it has advantage that is more grained than the q-hidden algorithm also this paper explains that ENP and hashing password is insecure and are easy to crack. It says that p-hidden algorithm is limited so that they utilize k-hidden with q-1 parameter**.**

3. Conclusion

Thus with all these existing paper the conclusion proceeds by combining many attacks together with three level security of the application. Added to this system, the paper includes upload of the file with encryption and decryption with can be loaded on to the cloud. This paper provides a safe and secured application for the user since all the personal details can ruin their life once it reaches the wrong one but the prevention helps the user to be more safe and secured in the application.

4. Scope for Future

The Implementation of this project with combination of attacks is to be made as a hybrid model. Thismodel can be used for other applications also. A common model should be adopted for implementing in the real server. An attempt is taken to combine SQL injection, DDOS and brute force attack together in the experiment.

References

[1] HimikaParmar, Nancy Nainan, SumaiyaThaseen, Generation of Secure One Time Password based on Image Authentication, CS & IT-CSCP 2012
[2] G. Sowmya, D.Jamuna, M.Venkata Krishna Reddy, Blocking Of Brute Force Attack, International Journal Of Engineering Research & Technology (IJERT) Volume 01, Issue 06 (August 2012).

[3] G. Sowmya, D.Jamuna, M.Venkata Krishna Reddy, Blocking Of Brute Force Attack, International Journal Of Engineering Research & Technology (IJERT) Volume 01, Issue 06 (August 2012).
[4] Pandey, Anand. (2015), Password Management Using OTP Authentication, International Journal of Advanced Research In Engineering Technology & Sciences. 2.101-105.
[5] Chithra, S., and E. George Dharma Prakash Raj, Overview of DDOS algorithms: A survey, International Journal of Computer Science and Mobile Computing IJCSMC 2, no. 7 (2013): 207-213.
[6] Dave, KonarkTruptiben, Brute-force Attack Seeking but distressing, Int. J. Innov. Eng. Technol. Brute-force 2, no. 3 (2013):75-78.
[7] Pooja, Monika, SQL Injection: Detection and Prevention Techniques, International Journal of Scientific & Engineering Research, Volume 7, Issue 12, December-2016 280 ISSN2229-5518.
[8] Agrawal, Surabhi, and Upendra Singh, Prevention of SQL Injection Attack in Web Application with Host Language, (2017):1468-1470.
[9] RudreshGurav, LeenaDabhade Mr. AbhilashKulkarni, Amar Agarwal, Rahul Chinchore, Personal Information in Passwords and Its Security Implications, International Journal of Advance Research in Science and Engineering,vol.07,Issue.05,March2018
[10] S.Soundharya, K.RaviKumar, Botnet Detection Technique Using Denial of Service (DDOS) Attack Elliptic Curve Digital Signature (ECDSA) Algorithm, International Journal of Research in Advent Technology, Vol.6, No.8, August 2018
[11] Luo, Wenjian, Yamin Hu, Hao Jiang, and Junteng Wang, Authentication by encrypted negative password, IEEE Transactions on Information Forensics and Security 14, no. 1 (2018):114-128.
[12] SachinJadhav, Sana Jamadar, PoojaLande, &Gayatri Mane. (2019), A NovelAuthenticationFramework Using Negative Password Method for Improving Security, Journal of NetworkSecurity Computer Networks, 5(1), 1–7.
[13] Salwa, P. B., and Nice Mathew, Encrypted Negative Password Using RSA Algorithm, (2019).
[14] Poornima S, Nivetha M, Pradeep Kumar M, Subathra S, Authentication by Encrypted Negative Password, International Journal Of Engineering Research & Technology (IJERT) RTICCT – 2020 (Volume 8 – Issue12),
[15] Mathew, JittyMerin, Bibin Varghese, and Smita C. Thomas, Password Authentication Framework Based on Encrypted NegativePassword, International Journal Of Innovative Science And Research Technology (IJISRT), Volume 5 - 2020, Issue 3
[16] S.Hema Kumar, J.UdayKiran, V.D.AKumar, G.Saranya, Ramalakshmi V.Effective OnlineMedical Appointment System.International Journal of Scientific & Technology Research , Volume 8, Issue 09, September 2019, Pages 803 – 805.
[17] Ramya,T.,Malathi,S.,ratheeksha,G.R. and V.D.Ambeth Kumar (2014). Personalized authentication procedure for restricted web service access in mobile phones.Applications of Digital Information and Web Technologies (ICADIWT), 2014, Page(s):69 - 74, Bangalore, India (ISBN:978-1-4799-2258-1)