# A survey on online banking authentication and data security

Stud.Ranjana Singh, AS.prof Kirti Patil, AS.Prof Ashish Tiwari

*Software System, Vindhya Institute of Technology & science*
*Umrikheda, Khandwa Road, Indore, Madhya Pradesh 452020*

***Abstract***— now in these days the internet users are increases in addition of that for providing the solutions different organizations are also provides their services online.The online service management and distribution need to preserve the sensitive information such as banking, online shopping applications. In these services the information security and authentication is a key aim of application design. In this presented work the online banking security is investigated and a review on the existing techniques of security and authentication is reported. Moreover a new design of the banking security and authentication is also provided which ensure the user and banking server to access the correct information by the correct person.

***Keywords***— online banking, cryptography, authentication, data security, network security

## I. Introduction

Internet technology leads to serve a large number of services for our daily routine such as email, messaging, social networking and others. Among these applications banking applications are one of most frequently used application and also carries a significant amount of sensitive data and private data. But there are various security issues in existing domain of banking data security and authentication. Some terms such as phishing, man in middle attack and other concepts of hacking and creaking are violate the privacy and security of user data and information.

On the other hand the security in the current banking system having some lakes which is desired to improve is listed below:

1. **Less secure authentication technique:** the authentication system consumes weak attributes for performing end client authentication, therefore security during authentication management is poor, thus desired to improve the authentication technique.
2. **Computationally expensive cryptographic approach:** the implemented cryptographic techniques are computationally fragile and consume higher space and time complexity for encrypting fewer amounts of data thus desired to improve the efficiency of implemented cryptographic techniques.

A number of security techniques are developed in recent years which protect the data in network and provide the authentication management. In these techniques computationally expensive algorithms and protocols are implemented for securely data transmission in network such as RSA algorithm which consumes more time when the data is transmitted at the server end. Therefore in this presented work a lightweight and efficient algorithm with complicated manner is provided for improving security and enhancing the performance of authentication. Additionally a new kind of security integration is desired which improve the computational cost and delay in network during the authentication process by efficiently applying the security techniques and improving the security in layered architectures.

## II. Related work

The given section provides the recently developed approaches for improving the security and authentication processes. Therefore a review of different research papers and article is provided.

The Electronic banking and payments service offering various financial services through the internet. To protect customers' information and identities over internet, necessary and standard multifactor authentication measures should be in place to avoid financial issues. The purpose of ***O.B. Lawal et al [1]*** is to find out the multifactor authentication (MFA) methods for banks, more over evaluate the type of security adopted and develop security measures to reliable authentication of customers remotely. The study addressed risk-based assessments and customer awareness programs to prevent the financial losses. The study was conducted on twenty (20) currently operating commercial banks in Nigeria.

Multi factor authentication based on one time password is utilized in variousapplications because of its security. However, existing OTP schemes suffer from several drawbacks because of weakness in hardware devices i.e. token devices that apply OTP schemes or because of the use of weak algorithms to generate OTP. A novel authentication scheme based on OTP is presented by ***Khalid Waleed Hussein et al [2]***. The scheme generates OTP based on unique numbers in addition to the usersbehavioural biometric. The purpose of the system is to make OTP more difficult, for restricting unauthorized access. The system ensures that the user who misuses the system is made liable. Therefore, the system is fit for fields that require high security guarantees, such as e-banking systems, and e-commerce systems.

***K.Thamizhchelvy et al [3]*** propose a Message Authentication Image (MAI) algorithm. This algorithm used to protect e-bankingagainst frauds such as Phishing and man-in-the-middle attacks. This Algorithm provides confidentiality, authentication and digital signature which is based on both Cryptography and Steganography to embed data in image. Algorithm generates fractals and embeds the password using chaos technique.

Two-factor authentication schemes aim at reinforcement the security of password-based authentication by secondary authentication tokens. Additionally 2FA schemes require no additional hardwareto store and handle secondary authentication token. That is also hence reasonable trade-off between security, usability and costs. These techniques are widely used in online banking. ***Alexandra Dmitrienko et al [4]*** investigate 2FA implementations of several well-known Internet service providers such as Google and Facebook. They identify various issues that allow attacker to bypass security, even when secondary authentication token is not under attacker's control. Then authors present a more general attack against mobile 2FA schemes. Attack relies on cross-platform infection that subverts control over both end points i.e. PC and mobile, involved in authentication. Authors apply this attack and successfully avoid diverse schemes: SMS-based TAN solutions, one instance of a visual TAN scheme, 2FA login verification systems of Google and Facebook accounts. Finally, cluster and analyse hundreds of real-world malicious Android apps that target mobile 2FA schemes and show that banking Trojans already deploy mobile counterparts that steal 2FA credentials like TANs.

Although branchless banking systems have spread to different parts of the world, methods to ensure transactional security in these systems have seen slower adoption because of a variety of operational constraints. A basic requirement from such systems is the provision of secure and reliable receipts to user's transactions, and recent attacks have demonstrated that existing systems fall short of fulfilling this requirement.***SaurabhPanjwani et al [5]*** propose a simple and practical protocol to enable users to authenticate transaction receipts in branchless banking. Given protocol usage missed calls from users to bank to distinguish real receipt and can be implemented on any mobile phone. Besides preventing spoofing attacks, the protocol enjoys significant advantages of usability, efficiency and cost, which make it a more practical choice than other schemes. Authors also discuss ways to use missed calls to mitigate man-in-the-middle attacks on branchless banking.

***A.SaiSuneel et al [6]*** describe the ATM which provides customers with convenient banknote trading are very common. A lot of criminals tamper with the ATM terminal and steal user's credit card and password by illegal means. Once user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time. How to carry on the valid identity to customer becomes the focus in current financial circle. Traditional ATM systems authenticate generally by using the credit card and password, the method has some defects. Using credit card and password cannot verify the client's identity. So there is a necessity to increase the security that customer use the ATM machine. So to rectify this problem author's aim to make ATM machine with more security by dual security i.e., fingerprint recognition and password without using ATM cards. Once the finger details are given and password is entered. Person can enter the amount to withdraw.

Necessity of e-banking, and their importance and role in decreasing distances and increasing service providing speed is obvious but impose many challenges to executives. Prevailing over people's distrust to the internet is one of these challenges that could be achieved with assuring security and privacy of user in internet and reducing faults. At the other hand, providing all infrastructures and tools needed in e-banking area violate cost limitations and require a great part of overall budget. Cloud computing is one of technologies that provide scalable and flexible resources via internet – that could be accessible everywhere – using pay-for-per-use approach, and have a great role in reducing businesses' information technology costs. ***Ali Abdollahi et al [7]*** a Single Sign-On(SSO) based integrated model for e-banking services is proposed that besides assuring more security, and reducing costs using cloud computing services, provides centralized management, simplicity and reduced faults.

Online banking allows consumers to access their banking accounts, review recent transactions, request statement, transfer funds, view current bank rates and product information. These services are offered by online banking are changing and being improved because of the intense competition between the banks. The major concern in online-banking is security specially user authentication. Banks use either symmetric or asymmetric cryptography for this but due to the advent of cryptanalysis techniques; security solutions are not much secure. Thus***Anand Sharma et al [8]*** isanalyse use of quantum cryptography for authentication purpose.

## III. Online banking issues

Banking via the Internet is an easy way to monitor your business's finances, allowing you to view payments and deposits on demand. This easy access to financial accounts makes Internet banking a common target for hackers and other online criminals, however. Understanding the security issues relating to Internet banking can help you keep both your personal and business accounts safe from intruders [9].

### *Password*

The key to protecting your Internet banking account is protecting your password. Using a strong password -- one that contains mixed-case letters, numbers, and even symbols if the bank allows it -- will decrease the likelihood of a hacker cracking the password and gaining access to your account. You should also ensure that the password to access your company's accounts is not the same as any other password you use, since not every site maintains the same level of security a bank does. If a hacker manages to steal a password from an insecure site, he can access any account that password unlocks.

### *Phishing*

One of the primary methods a hacker gains access to account information is through phishing, or tricking the victim into giving up the information voluntarily. A hacker might send an e-mail or even call, pretending to be a representative of the bank and informing you about some irregularities with your account. All you need to do to sort things out is to provide your password or other account information to verify your identity. If you ever receive a communication that appears to be from your bank and requests this type of information, contact your bank by phone immediately. Do not give out account information to a caller, and do not click any links provided in any e-mails that claim to be from your bank. You should also ensure that any employees with access to the company's accounts follow the same procedures.

### *Keyloggers*

Keyloggers are malware programs that record keystrokes and other data, allowing a hacker to capture your password as you enter it. Maintaining up-to-date antivirus suites on your company computers can prevent these malicious programs from gaining a foothold, and setting up your network's firewall to monitor outgoing traffic can help you determine when an infection occurs. Many keyloggers and viruses use email to travel from computer to computer, so adding anti-virus protection to your company's email server can help filter out these attacks.

Therefore a potential method is required to develop a suitable and secure technique by which the banking applications are providing the services in more secure and effective manner. Thus the proposed study is focused on developing a secure cloud based solutions for improving the current banking security improvements. This section provides the formal overview of the proposed work. In the next section the motivation of the proposed work is discussed.

## IV. PROPOSED WORK

On line banking provides more convenient methods for providing banking services. In order to providing security in such systems there are a number of techniques available. But these techniques having some deficiencies' some of them targeting in this proposed study is givens as:

1. **Less secure authentication technique:** the authentication system consumes weak attributes for performing end client authentication, therefore security during authentication management is poor, thus desired to improve the authentication technique.
2. **Computationally expensive cryptographic approach:** the implemented cryptographic techniques are computationally fragile and consume higher space and time complexity for encrypting fewer amounts of data. Thus desired to improve the efficiency of implemented cryptographic techniques.

In order to develop a secure authentication and cryptographic technique the following task are incorporated with the system.

1. **Implementation of hardware attributes based authentication system:** the proposed authentication system is a tree phase authentication system, which involve the following steps of authentication.
    a. Hardware authentication
    b. One time password and strong password management
    c. Security answering
2. **Implementation of lightweight cryptographic algorithm for efficient encryption and decryption:** in order to develop the lightweight hybrid cryptographic technique the following algorithms are hybridized.
    a. ECDH
    b. MD5

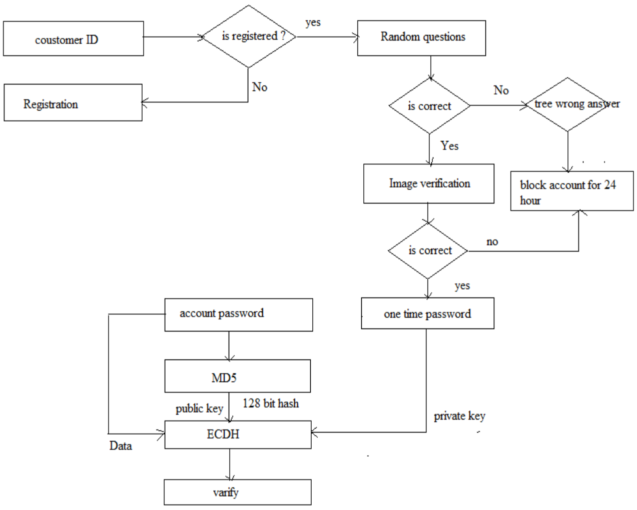

Figure 1 proposed system

The proposed working model and their involved processes are given in the above given diagram in this diagram a number of sequential processes are taken place. First user provides their ***customer ID*** for initializing the authentication process if user is not nonregistered then system redirect the user for ***registration process***. Otherwise system generate random question which is submitted previously during registration process. The ***randomly generated question*** can be a date of birth, PAN card detail or any user sensitive information. Is user answer all the questions than the systems ask for image authentication during this process images with tags are appeared and required to select correct image and tag for successful authentication. As the user select the correct image and tag a one-time password is sent to the user mobile and this one time password is used as public key for encryption. In addition of that user provides the password which is first produced into the MD5 algorithm for hash key generation. This hash key is used as private key for encryption algorithm. Then the generated public key and private key with the password as data is transmitted to the server for verification.

## V. Conclusions

The given paper provides the detailed study on online banking. In addition of that different research and security issues concerned with the current online banking is also reviewed. In order to find an adoptable solution some pre-existing models recently developed is also reviewed. Finally some key issues are addressed on which the solution is needed to find. Therefore for resolving the issues a new security and authentication model is proposed for implementation in near future.

## References

[1] O.B. Lawal, A. Ibitola, O.B. Longe, "Internet Banking Authentication Methods in Nigeria Commercial Banks", African Journal of Computing & ICT, Vol 6. No. 1, March 2013

[2] Khalid Waleed Hussein, Nor FazlidaMohd. Sani, RamlanMahmod, Mohd. Taufik Abdullah, "Active Authentication by one Time Password Based on Unique Factor and Behavioral Biometric", International Journal of Computer Networks and Security, ISSN: 2051-6878, Vol.23, Issue.2

[3] K.Thamizhchelvy, G.Geetha, "E-Banking Security: Mitigating Online Threats Using Message Authentication Image (MAI) Algorithm", 2012 International Conference on Computing Sciences, 978-0-7695-4817-3/12 $26.00 © 2012 IEEE

[4] Alexandra Dmitrienko, Christopher Liebchen, Christian Rossow, Ahmad-Reza Sadeghi, "On the (In)Security of Mobile Two-Factor Authentication", TechnischeUniversit¨at Darmstadt Center for Advanced Security Research Darmstadt D-64293 Darmstadt, Germany, First Revision: January 31, 2014

[5] SaurabhPanjwani, "Practical Receipt Authentication for Branchless Banking", DEV '13, January 11-12, 2013 Bangalore India Copyright c 2013 ACM

[6] A.SaiSuneel, S.B.Sridevi, K.Nalini, "Dual Security Using Fingerprint and Password in Banking System", International Journal of Review in Electronics & Communication Engineering (IJRECE) Volume 1 - Issue 3 August 2013

[7] Ali Abdollahi, Mehdi Afzali, "A SINGLE SIGN-ON BASED INTEGRATED MODEL FOR E-BANKING SERVICES THROUGH CLOUD COMPUTING", International Journal of Advances in Computer Science and Technology, Volume 3, No.1, January 2014

[8] Anand Sharma, S.K.Lenka, "Authentication in Online Banking Systems: Quantum Cryptography Perspective", International Journal of Scientific & Engineering Research, Volume 5, Issue 2, February-2014

[9] Milton Kazmeyer, "Security Issues Relating to Internet Banking", http://yourbusiness.azcentral.com/security-issues-relating-internet-banking-21683.html