International Journal of Research in Engineering, Science and Management
Volume 8, Issue 4, April 2025
https://www.ijresm.com | ISSN (Online): 2581-5792

Advance Mobile OTP Concept for Online Money Transaction

Shashi Kant Pal[1*], Kavita[2]
[1]M.Tech. Student, Department of Computer Science, Shri Venkateshwara University, Meerut, India
[2]Shri Venkateshwara University, Meerut, India

***Abstract*: Online banking and money transfer mostly based on OTP to provide two step verification and security but still there are chances of OTP being attacked via SIM swap, smart phone Trojan plantation, now a days OTP system is also vulnerable. There is enhanced security feature option where we can design OTP for banking where we can secure it to the next level for money transfer. In case normal OTP get compromised by any way but still that would be challenging for the unauthorized person to decode the OTP for illegal transaction.**

***Keywords*: OTP, Code sheet, MITM, Cryptography, Secure Code, Salting, Authentication, Transaction, Online Banking, Server, Database.**

1. Introduction

Banking and online money transfer with OTP authentication process will be stronger, it can be designed advance OTP concept using salting and user-based coding, defined on OTP server and integrated with online banking and to provide end user level of OTP salting with encoded logic and code sheet.

Define OTP example 4 Digit and salting (encoded) value for 4 Digits, Server will send 4-digit code where in response user will merge salted (encoding) code with OTP as per defined for his/her OTP system.

End user can opt for the security for his profile as per the complexity requirements.

Levels for 4-digit OTP example: X= OTP numerical digit (Variable), U = user defined numerical number/symbol /character (Fixed Value)

1. OTP 4 Digit XXXX, where user can choose salting place and value (0-9, A-Z, symbols), i.e UXXXX, XUXXX XXUXX, XXXUX or XXXXU.
2. Same as one and define double position of U i.e., (UUXXXX, UXXXUX, XXXXUU, UXXXXU, XXUUXX)
3. Bank will Generate Secure code for numbers 0-9 and customer will salt(encode) his fixed value in OTP place.
   Example – 0 – $P, 1 – %1, 2 – &^, 3 – V(, 4 – L$...up to 9 digit etc.
4. Same as User defined Salt with code between 1 to 4 position and so on value for 0-9 for user secure code like below:

Example: 1 - X2#, 2 – 3!, 3 – A2, 4 - & ……etc.

Once user receives OTP with random number, will use that secure code sheet provided by Bank and salt his\her own fixed value in response. Secure code sheet can be updated on regular interval and provided with unique code book for every customer at the time of Bank Account Opening and users can also modify and update their code when required. This complexity level can be chosen as per end user convenience and requirements.

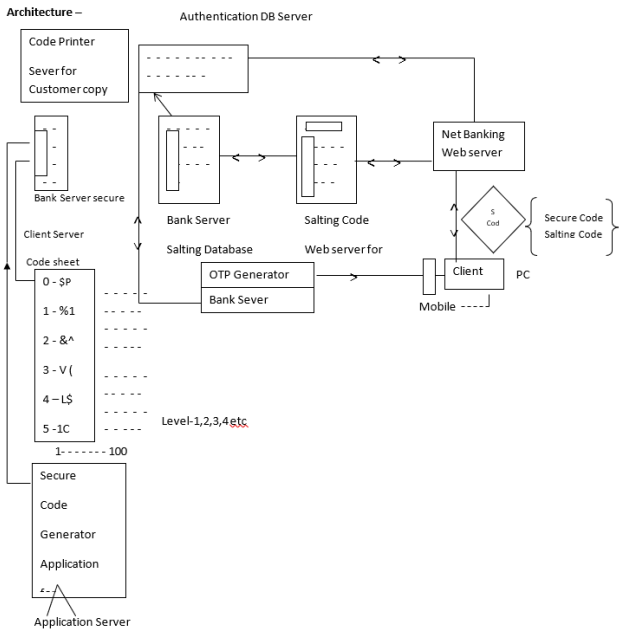

Fig. 1.

Practical Test – User can set salt value on position 2 for one Salt character and take defined value as 3!. User gets OTP during money transfer as 1234, in OTP response value would response as per Level 2 chosen %13!&^V(L$ as per below image. Example:

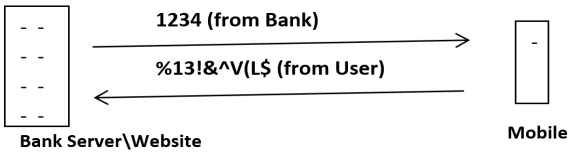

Fig. 2.

*Corresponding author: shashikantpal@gmail.com

Secure Code (Bank Defined) - 1 – %1, 2 – &^, 3 – V(, 4 – L$
User Salt Code (User Defined) - 1 - X2#, 2 – 3!, 3 – A2, 4 - &

A. Define Bank OTP (Variable Value) and User (Fixed Value)

OTP size will be 4 digit or more, can be designed and defined as per the security requirement and feasibility of the database system in order to increase security. Position of the User defined value and place will make system more complex and tough to crack the OTP code for attackers. Database and data transmission will take place in secure mode with encryption.

B. End User to Set Fixed User's Value in OTP Definition

User set the OTP definition where select the level of complexity like 1-to-4-digit position as per user defined value and then select the position of his salt code value in OTP response. User can define one to two places of total length of OTP in response during OTP return.

C. OTP Server Code Generation and Response from User

OTP server will generate the random number and will send the code to user on phone or email. After receiving the code user will add his defined salt code (s) on the position of OTP and put in the banking transaction portal. OTP server will match the code with its database and authenticate once the code will be matched.

2. Conclusion

Advance Security of the Online Banking and Money Transaction System – This Banking advance OTP system will provide enhanced feature to secure OTP return code from MITM attack, SIM swap\cloning, planted Trojan attack on smart phones, if Server generated OTP will be exposed to attacker, they will not be able to match the user defined code and position or bank secure code. This OTP based on salting code and bank referential code; it would be tough to crack for unauthorized person.

References

[1] https://economictimes.indiatimes.com/news/politics-and-nation/new-form-of-otp-theft-on-rise-many-techies-victims/articleshow/67521098.cms
[2] https://economictimes.indiatimes.com/industry/banking/finance/banking/no-otp-is-not-surefire-protection-against-online-banking-fraud/articleshow/66236191.cms
[3] https://en.wikipedia.org/wiki/Salt_(cryptography)
[4] https://en.wikipedia.org/wiki/One-time_password
[5] Manisha M. More, Meenakshi P. Jadhav and K.M. Nalawade, (2015), "Online Banking and Cyber Attacks: The current Scenario," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, no. 12, pp. 743-749.
[6] Soni R.R and Soni Neena (2013), "An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks," Research Journal of management Sciences, vol. 2, no.7, pp. 22-27.
[7] Mohd Khairul Ahmad, Rayvieana Vera Rosalim, Leau YU Beng and Tan Soo Fun (2010), "Security issues on Banking Systems," International Journal of Computer Science and Information Technologies, vol. 1, no.4, pp. 268-272.
[8] Navjeet Kaur, (2015), "A Survey on Online Banking System Attacks and its Countermeasures," International Journal of Computer Science and Network Security, vol.15, no.3, pp. 57-61.
[9] Susheel Chandra Bhatt and Durgesh Pant (2011), "Study of Indian Banks Websites for Cyber Crime Safety Mechanism," International Journal of Advanced Computer Science and Applications, vol. 2, no. 10, pp. 87-90.