# Secure OTP with Salting System for Banking

Shashi Kant Pal

*SME (Windows Server), Department of Information Technology, IBM India Pvt. Ltd., New Delhi, India*

***Abstract*****: Online banking login and transaction system is using OTP to provide two step verification and security but still there are chances of OTP being attacked via SIM swap, smart phone Trojan plantation and over email OTP system is also vulnerable. There is enhanced security feature option where we can design OTP salting defined by OTP banking server on which user can choose level of OTP salting and use with the real time OTP in order to do secure transaction. In case attacker get the OTP but they will be unable to identify the salt code to mix with OTP for further transaction.**

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

## 1. Introduction

To make Online Banking System or Authentication Process more strong, we can design secure OTP system using salting, define on OTP server and integrated with online banking and give user level of OTP salting as per below logic which would also be easy for the users to remember.

Define OTP 2-4 Digit and salting value of 2-4 Digits, Server will send 2-digit code where in response user will merge salted code with OTP as per defined for his/her OTP system.

Server Side Definition which user can choose as per security requirement and suitability for his profile.

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), UXXX, XUXX, XXUX or XXXU.

2 - Same as 1 and define double position of U (UUXX, UXUX, XXUU, UXXU, XUUX)

3- Bank will generate secure code for numbers 0-9 and customer will salt his fixed value in OTP place.

Example – 0 – A!, 1 – C@, 2 – T%, 3 – $Q, 4 – (% etc.

4- Same as 3 with variable code between 1 to 3 value for 0-9 for user secure code like below:

0 - A^, 1 - X2#, 2 – 3!, 3 – A2, 4 - & ……etc.

Once user receives OTP with random number he/she 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 customer skill and requirements.

## 2. Test and Results

Suppose user set salt value on position 2 and take defined value as e. He/She gets OTP during money transfer as 1234, in OTP response value would response as per Level 4 chosen X2#e3!A2&

Length of OTP (variable value) and User Defined (fixed value) – Length of OTP size more than 4 digit, 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.

### *A. USER to Generate Salted OTP definition for his/her profile*

New user will login into the banking portal and go to the OTP definition where select the level of complexity like 1-4 digit user defined value and then select the position of his value in OTP response. User can define maximum 50% of total length of OTP in response.

### *B. OTP Server Code Generation and Response from user*

OTP server will generate the maximum 50% of the random number will send the code to user on phone or email. After receiving the code user will add his defined code (s) on the position of OTP and put in the banking transaction portal. OTP server will match the code with it’s database and allow once the code will be matched.

## 3. Conclusion

Security of the System – This system will provide enhanced feature to secure code from MITM attack, SIM swap\cloning, planted Trojan attack on smart phones, if Server generated OTP is exposed to attacker they will not be able to match the user defined code and position or bank secure code easily. This OTP based salting feature would almost be tough to crack until attacker hack the OTP Database or banking servers.

## 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