OFFLINE MOBILE BASED OTP TECHNOLOGY FOR ENTERPRISE IOT ENABLED ARCHITECTURE IN BANKING CASH LOGISTICS & ATM OPERATIONS

Lebbaeus Denis
Research Scholar, Bharath Institute of Higher Education and Research (BIHER), Chennai, India

Dr. T. Krishna Kumar
Assistant Professor, Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research (BIHER), Chennai, India

Dr. Karthikeyan
Professor and Principal, Department of Computer Science and Engineering, Tamilnadu College Of Engineering, Coimbatore, India

Dr. S. Sasipriya
Professor, Department of Electronics and Communication Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India

ABSTRACT

The Internet has been in presence for more than 40 years now and the expression "Internet of Things" (IoT) has been being used since huge scale appropriation of RFID started 10 years back. IoT empowers things to convey about themselves and their condition with different things and PCs and enable them to take an interest in business procedures and regular day to day existences of individuals. Many financial frameworks have fulfilled the 2FA necessities by sending a One Time Password (OTP), something had, through a SMS to the client's telephone gadget. Unfortunately, universal roaming and SMS expenses and delays put restrictions on this system reliability. It gives a stage to correspondence between objects where items can compose and oversee themselves. By analyzing current technology research and by investigating future application situations for the Internet of Things, this paper will feature out its potentially huge advantages in the cash logistics and ATM operations.

Keywords: ATM, OEM, IoT, OTP, Automated Teller Machine
1. INTRODUCTION

The application will replace the need for receiving the OTP for Internet Banking transactions via SMS. OTP can be produced utilizing the application after it is enlisted. SIM card is not needed for Offline OTP. The application will give OTP Internet availability when Online OTP is picked. At the point when the web availability isn't accessible in portable the Offline OTP alternative can be utilized.

The application will be available in the marketplace of Android in Phase 1 and later in Phase 2. The app will also be made available for iOS, Windows and Blackberry. The Customer will be required to select "Online" option in the Internet Banking Portal in the transaction confirmation page and select "Online OTP" Service Activation along with Secure OTP app also to generate the OTP.

If the customer selects "Offline" in the Banks Secure Portal in the exchange confirmation page, an irregular number will be appeared in the following page where OTP is to be entered, wherein the client can choose "Disconnected OTP" in the Bank Secure OTP application. What's more, enter the arbitrary number in the Bank Secure OTP application and create an OTP.

2. RELATED LITERATURE SURVEY

The Mobile App on the Offline mode can be manufactured dependent on Time-based One-time Password Algorithm (TOTP)
TOTP is a case of a hash-based message validation code (HMAC). It consolidates a mystery key with the current timestamp utilizing a cryptographic hash capacity to create a one-time secret phrase. The timestamp normally increments in 30-second interims, so passwords created near one another in time from a similar mystery key will be equivalent.

In a regular two-factor check application, customer affirmation proceeds as seeks after: a customer enters username and mystery word into a site or other server, delivers a one-time mystery key for the server utilizing TOTP running locally on an advanced mobile phone or other gadget, and types that secret phrase into the server too. The server by then in like manner runs TOTP to check the entered one-time mystery key. For this to work, the tickers of the customer's device and the server ought to be commonly synchronized (the server will typically recognize one-time passwords created from timestamps that difference by ±1 time between time from the client's timestamp). A singular puzzle key, to be used for all resulting approval sessions, almost certainly been shared between the server and the customer's device over an ensured channel early. In case some more advances are done, the customer can moreover affirm the server using TOTP.

3. PROJECT SOLUTION
3.1. SHA256 Algorithm
SHA-256 calculation is fundamentally the same as in structure to SHA-1, yet in addition to the fact that it uses eight, instead of five, 32-piece sub blocks, however there are different manners by which it isn't practically equivalent to. For SHA-256, the message is cushioned, and separated into 512-piece hinders, similarly with respect to SHA-

Notes on the execution of the preprocessing stage
- FIPS 180-4 demonstrates message has a '1' piece included, then padded to a sum number of 512-piece checking the length of the message in the last 64 bits of the last block.
- As we hold a byte-stream or possibly than a small stream, including a byte '10000000' (0x80) includes a necessary piece "I".
- To change over the message to 512-piece squares, I figure the quantity of pieces required, N, by then for every one of these I make a 16 whole number (for example 512-piece) group. For each on the off chance that these integrability.
- The charCodeAt() procedure send NaN for beyond the field of play, however the '1' head changes over to 0, so the 0-cushioning will be done unquestionably change into block.
- Thereafter the message length (in bits) should be included in the 64 bits, which should be the last two integrability in the last square.
4. PROPOSED SYSTEM

4.1. System Design Methodology

In this paper, I propose an Offline versatile based OTP for Banking Cash Logistics and ATM Operations. This should supplant existing innovation. The Server will produce a Secured OTP utilizing SHA256.

4.2. OTP Algorithm

The delivered OTP must be outcome as a figure for the checking process which is pursued by software engineering In like manner, it is basic to develop an ensured OTP making count. A couple of parts can be used by the OTP estimation to make a difficult to-figure mystery state Hence the secured OTP process performed by the SHA256 Algorithm.

The excellent OTP is delivered by the versatile application detached, without interfacing with the server. The PDA will use somebody of a sort information to deliver the mystery word. The server will use a comparative stand-out information and endorse the OTP. All together for the structure to be secure, the novel OTP must be hard to envision by developers. The going with parts will be used to make the OTP.

Number IMSI: The International Mobile Subscriber Identity term speaks to an uncommon number related with all Universal Mobile Telecommunications System (UMTS) and GMS organize phone customers. It is taken care of in the (SIM) card in the PDA. The server Data based will be under secured by these numbers.

4.3. OTP Offline OTP proposed System- Technology Architecture

ATM PIN: In case the phone is taken, without knowing the customer's PIN a genuine OTP can't be made. It is simply being used particularly to make the OTP and obliterated after that.

Timestamp: Used to make momentous OTP, real for a short proportion of time. One of the servers must be synchronized with the timestamp on the phone.

DOB: DOB of customer who is going to use the app.

Username: Name of the custodian given by the bank.
Offline Mobile Based OTP Technology for Enterprise IOT Enabled Architecture in Banking Cash Logistics & ATM Operations

**Figure 1** Shows menu to generate OTP (IMSI No. taken automatically)

**Figure 2** Shows how OTP generated in Android mobile.

*How OTP Generated*

The Name, secret key, DOB of overseer is given from the server and then linked with the present date, time and the time stamp which is substantial. This connected string is then given as contribution to Secured Hash Algorithm (SHA256) calculation. SHA-256 calculation restores its message digest which is 20 bytes esteem. The 20 bytes will be decreased to 5 bytes by XOR operations.

By then from this 5 byte respect, each byte is correct moved with 4 digits and after that is changed over to hexadecimal. Finally by changing over the ASCII regards to a character string, it is appeared as an onetime mystery expression to the overseer.

*4.4. Database Design*

The A info is needed on the server aspect to store the regulator’s ID info, as an example, the essential name, last name, username, mystery key and also the organiser variety for every superintendent. The OTP field can store the hash of the ten minute just once word. It will not store the OTP itself. ought to the info be undermined the hashes cannot be convoluted so as to urge the OTP accustomed deliver those hashes. during this manner, the OTP count will not be pursued.

http://www.iaeme.com/IIARET/index.asp editor@iaeme.com

Electronic copy available at: https://ssrn.com/abstract=3526855
5. BENEFITS

- Reduced cost of operation - due to less charge in Alternate Banking Channel.
- BANK AT HOME - by HNI, Young generation and Corporate.
- NIIM would be in ascending order as this process would facilitate to increase in CASA.
- Specialized would be given to clause clients as foot fall in the Branch would be reduced.
- Increase in CASA customers would enhance the Cross selling of Retail Business and Associate Products
- Non availability of Internet connection.
- No Hardware facility is required in the Institutions
- Tech savvy people viz Young generation, HNI,NRI and Big Corporate would come to our fold.
- IMB coverage is less than 7% (Ref The Hindu –Tamil daily dt 05 09 2016). Potential to increase segment
- Charges for Internet facility are available at cheap price. Eg. Reliance. – Hence augmentation is very easy.
- Hardware and Internet facility are available at cheap cost.
- Customers who were not using facility would also be inclined to use this facility as the cost is less.

6. OUTCOMES

![Login Screen](https://ssrn.com/abstract=3526855)

**Figure 3** Login Screen
Offline Mobile Based OTP Technology for Enterprise IOT Enabled Architecture in Banking Cash Logistics & ATM Operations

**Figure 4** New Registration Screen and New Reg OTP approval screen

**Figure 5** m Pin entry Screen and offline m pin Change Screen

**Figure 6** Online Generated and Offline generated Screen using Trans ID

http://www.iaeme.com/IJARET/index.asp 67  editor@iaeme.com

Electronic copy available at: https://ssrn.com/abstract=3526855
Offline OTP: In the event of non-availability of mobile connectivity / wi-fi / Internet failure Secured OTP is generated duly combining the transaction id by the mobile user thru mobile app. and thus enabling the customer to process the transaction.

App will sync and identify the availability of network / internet connection, if both facility are not available, it will turn to offline mode by default and will seek for mPIN for login authentication, This mPIN will work only in the registered mobile.

The application validates the mPIN and moves to offline mode, and the user will generate the offline OTP duly validated with IMEI No with Encryption and Transaction ID which is provided in the net banking site by the bank server.

SHA128 Encrypted with added before salt and Salt should be generated using a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG), and Prepare the salt to the password and hash it with a standard cryptographic hash function - SHA256 and Save both the salt and the hash in the user's database record.

7. CONCLUSION AND FUTURE SCOPE

I considered the challenges of securing the passwords on the internet and shown some equivalent effort in this field. Also we have discussed how to secure OTP passwords which is generated by server. The advanced system reduced the difficulties of old PIN entry methods Also I have introduced a new PIN-entry technique that has proposed security against old method. This is feasible by successfully enlarging the part of memory.

REFERENCES

[1] Khan, Burhan, et.al. "Re Hashing Security System Solutions in Online-Banking." International Journal of Engineering & Technology 7, 2018

[2] Ashfield, James M, et.al. “Apparatus and Method for using a Portion of a One-Time Password as a Dynamic Card Validation Value.” October 25, 2016.

[3] Benson, Glenn S et.al. "System and Method for Anti-Phishing Authentication." U.S. Patent 9,374,366, issued June 21, 2016.
Offline Mobile Based OTP Technology for Enterprise IOT Enabled Architecture in Banking Cash Logistics & ATM Operations

[4] Varadarajan, Rammohan, et.al "One-Time use Password Process and Methods.", 2017.

[5] Syeda Kausar Fatima, Dr. Syeda Gauhar Fatima, Dr. Syed Abdul Sattar, and Dr. Anita Sheela, A Monitoring Scheme with IoT and Sensor Expertise, International Journal of Advanced Research in Engineering and Technology, 10(2), 2019, pp. 271-277

[6] Mardikar, Upendra S et.al.. "Biometric Authentication of Mobile Transactions by Trusted Service Managers. 2018.

[7] Cobourne, Sheila. et.al "Challenging Environments Using Mobile Gadgets for Security." 2018

[8] Bond, Michael K., et.al "CRM Security Core.", 2017.

[9] Essebag, Jacques, et.al "Method for a Prepaid, Credit Card Debit and Security Code Generation System." 2018.

[10] Dr. Raju Anitha, S. Harsha Vardhan, Ch. Akhil and G. Sona, An Automated SMS-Update System through IoT using Raspberry Pi, International Journal of Mechanical Engineering and Technology 9(1), 2018, pp. 118–124

[11] Eisen, Ori. "Systems and Methods for Detection of Session Tampering and Fraud Prevention." 2018.

[12] Cady, et.al Stems and Methods for Mobile Device-Enabled Cardless Cash Withdrawals." 2019.

[13] Barnett, Timothy William, Alexander I. Kasatkin, Christopher Hozumi Miyata, and Daniel Ruehle. "Systems and Methods For Decryption as a Service Via a Message Queuing Protocol." U.S. Patent Application 10/027,635, filed July 17, 2018.

[14] P. Dayaker, Y. Madan Reddy and M Bhargav Kumar, A Survey on Applications and Security Issues of Internet of Things (IoT), International Journal of Mechanical Engineering and Technology, 8(6), 2017, pp. 641–648

[15] O'hare, Mark S., et.al "Secure Data Parser Process and Operation." April 3, 2018.

[16] Hammad, Ayman. "Integration of Payment Capability into Secure Elements of Computers." U.S. Patent 9,424,413, issued August 23, 2016

[17] B. Thamotharan, S. Ramakrishnan, A.N.S.P. Sharan and K. Rajesh, A Two Phase OTP Based Approach to Achieve Confidentiality, Integrity and Non-repudiation in Cloud, International Journal of Mechanical Engineering and Technology 8(8), 2017, pp. 951–957

[18] Hammad, Ayman, Patrick Faith, Krishna Prasad Koganti, Ben Rewis, Brendan Xavier Louis, Kevin Weller, and Benedicto Hernandez Dominguez. "Secure Authentication System and Method." U.S. Patent Application 15/690,150, filed January 4, 2018.

[19] L. Orsini, and Roger S. Davenport. "Authenticate data parser method and system." 2018