Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 04, April 2021: 2346-2358

Research Article

Multiple Service Authentication with Cloud OTP as a service

L.Raji[1], T.Sona[2], J.Varshini[3], B.V.Sravani[4]

[1,2,3,4]Department of Computer Science and Engineering, R.M.K Engineering College, Chennai-601206, India

Abstract

An OTP, or One-Time Password, is an extra security mechanism for online transactions that involves two-step authentication. For most financial transactions, this damn time OTP has become a very popular option. Because of its increasing popularity, it is becoming more accessible to fraudsters who try to steal your OTP in order to compromise your account or perform illegal financial transactions. The Proposed system provides a solution and works well as a multiple authentication security mechanism and has a lot of configuration options built in.This protects against a range of social, personalized, and opportunistic attacks.

Outsiders are unable to gain access to the cloud infrastructure unless the customer has correctly authenticated by the cloud service provider. The cloud offers four priority levels of security that would provide a strong barrier against unauthorized access to the user account. The Created Cloud Id, or UID, will play an important role in gaining access to the user's cloud account and to the applications utilized by the User. In terms of experience, professionals, resources, and firmware, the proposed framework allows businesses to spend very little on OTP - based TFA transfer. It also allows the user to manage multiple accounts from one location, and via unlikable profiles. It is thought that outsourcing OTP service to the cloud will make it easier for many cloud service providers to enforce bundle OTP because it does not demand extra investment.

Keywords: *Multiple factor authentication , OTP as a service , Priority level for security in cloud OTP ,Generate Cloud Token, Generate Unique Id , Generate Cloud Id*

Introduction

Since several web services began to connect, consumers found classic login credentials encryption is insufficient. Complicated attacks are aimed at the least effective of many of these digital credentials, and they are used to recover other credentials. One-time passwords, which are a two-factor authentication method, appear to be a natural enhancement over classical username and password schemes as developers look for new authentication mechanisms. The manuscript quickly moves the OTP verification to the cloud to make things easier for cloud

service providers to execute it. When the OTP verification is provided as a service in the cloud, other cloud service providers can delegate their OTP deployments, and cloud users can access their accounts with the OTP provider on various cloud services. This enables them to utilize multiple cloud providers without having to maintain multiple OTP accounts for service.

To streamline the multiple factor of authentication, the paper describes the architecture for building a stable, online privacy, and stream OTP service in the cloud. The phases of cloud registration process, service provider setup, and authorization are all examined. The proposed architecture's security and privacy considerations are described and evaluated. Extrovert attacks, contribute to the loss of user profile, attacks from suspicious service providers, and OTP verification are all minimized within the relevant information. As a result of the study, the proposed solution, which locates the OTP provider in the cloud, is made stable and safe.

Literature Survey

The project's necessary survey is focused on the field of "Cloud computing." As we all know, nowadays, everything is done over the internet. Human life has changed dramatically as a result of technological advancements. Multiple-factor authentication would be needed for online transactions. In online transactions, two-factor authentication is already possible. However, intruders continue to gain access and conduct transactions without the user's knowledge. What makes you think that's possible? "Third-party access, corrupt intruders, and Ignorance threats," was the response. Cloud storage is a new technology that allows you to share all of your tools, such as the internet, to store, access, and process data.

Infrastructure as a service (IAAS), Platform as a service (PAAS), and Software as a Service (SAAS) are all examples of cloud computing services . The project's main goal is to offer One Time Passwords as a service to cloud service providers' registered users.

2.1 Password Authentication Process

To protect users' privacy, user authentication is a critical subject in information security. To some extent, computer security is reliant on reliable user authentication. In the current state, there are numerous authentication schemes. These are focused on the user's biological and physiological features, whereas others, such as textual and graphical passwords, are based on the user's awareness.

Furthermore, some significant authentication models, such as smart cards, are dependent on what you've said.

Textual password and token-based authentication schemes, or a combination of both, are widely used by the various encryption designs. Both authentication patterns, however, are vulnerable to certain attacks, as discussed in the following section. To achieve high quality service, cloud computing makes use of low-power hosts. However, in order to provide secure application access in the Cloud computing environment, authentication is one of the most pressing issues.

2.2 Multiple Factor Authentication in Cloud Service

Multiple Factor Authentication (MFA) is a means of obtaining encrypted access to an application. From digital transactions to online chat, privacy and protection from intruders are expected. However, all cyber crimes are caused by a lack of key protection. As a result, multiple factor authentication is integrated into the cloud OTP service provider, and these authentication levels can differ based on the protection level required by the customer. OTP authentication, Captcha authentication, Cloud OTP authentication, and finally Cloud UID (Unique Id) and Cloud Token Verification are all part of this multiple-factor authentication. All of these types of authentication ensure that only the appropriate person have access to the application.

2.3 Generating Tokens and Unique Id for Users

When delivering a Cloud OTP service, we must create a unique identifier for each user in order to provide them with the required service. And therefore we must verify the information given by the user. In order to avoid any difficulties in serving them, details such as the user's email address and mobile phone number must be validated. As a result, the research has progressed to the point that each and every user will be assigned a Cloud Token and a Cloud UID. And we came up with the RSA Algorithm as a solution. It is the foundation of a cryptosystem and a set of cryptographic algorithms that allow public key encryption and are widely used to secure sensitive data, especially when it is
sent over an insecure network like the internet.

2.4 Security Level provided with priority

The research is going on to the next level in order to resolve the weaknesses of the existing method. The project's primary objective is to have a particular level of protection with a lower value. We want to integrate it into our real-time applications, such as chat, e-commerce, and banking.

We chose to provide a simple, conventional level of protection with one time verification for the Chat application because it does not require further security. Next, when we consider an e-commerce platform, it requires a slightly higher degree of security than a chat application, and authentication is required at all times. As you might be aware, bank applications need a higher

degree of security than other applications because all of our assets are connected to bank data. As a result, we intended to obtain user KYC information
in order to provide a high degree of protection to Bank users in the Cloud OTP service.

2.5 Drawbacks in Existing System

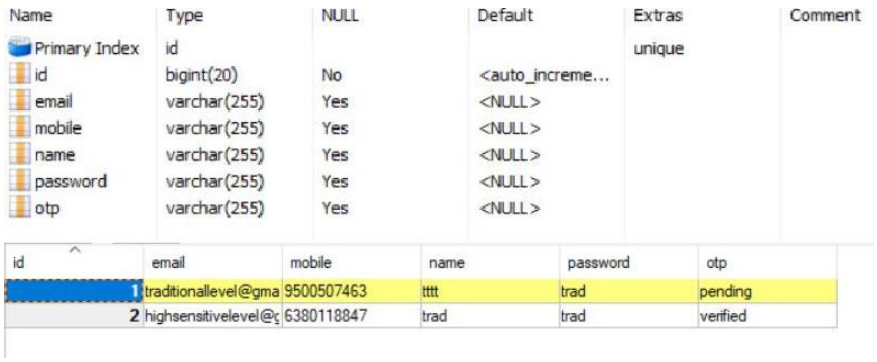
Complex attacks are aimed at the weakest of many of these online credentials, and online credentials are used to recover other credentials. Opposition to OTP replays and lightens attacks, third- party access, corrupted insiders, and Ignorance attacks are all possible. The cost of implementing OTP authentication in terms of manpower, equipment, and tools is higher on the developmental side.

Dataset

The datasets are the most essential aspect they can only assist us in finding the approved user. As previously mentioned, the data we provide differs depending on the security level. When a user registers for the first time, the four security levels will ask for information. If a user has registered, their data is automatically stored in a database and can be accessed using their cloud UID. In order to store and access data in the MySQL server, the Apache Tomcat and Hibernate platform is necessary. Hibernate is a Java framework that makes it easier to build database-interactive Java applications. It's an ORM (Object Relational Mapping) tool that's free software and flexible. Data development, data manipulation, and data access are all greatly enhanced with an ORM tool. It's a programming technique that links an object to data in a database.

3.1 Dataset required for Traditional security level

Only mobile number and an email address are required for the Traditional level of protection. The user must build an account on a cloud OTP service platform. The cloud will generate a cloud token, which will be sent to the user's registered email address. After entering the correct cloud token, the user can proceed to the next stage of verification, cloud OTP verification for the registered mobile number. The registered mobile number and email address are mapped in the Hibernate platform. After that, the user need to use this login credential to gain access to their chat application at all times. If the user uses a different set of credentials or someone else tries to log into user's account, they will be denied access to that application.



Name	Type	NULL	Default	Extras	Comment
Primary Index	id			unique	
id	bigint(20)	No	<auto_increme...		
email	varchar(255)	Yes	<NULL>		
mobile	varchar(255)	Yes	<NULL>		
name	varchar(255)	Yes	<NULL>		
password	varchar(255)	Yes	<NULL>		
otp	varchar(255)	Yes	<NULL>		

id	email	mobile	name	password	otp
1	traditionallevel@gma	9500507463	tttt	trad	pending
2	highsensitivelevel@g	6380118847	trad	trad	verified

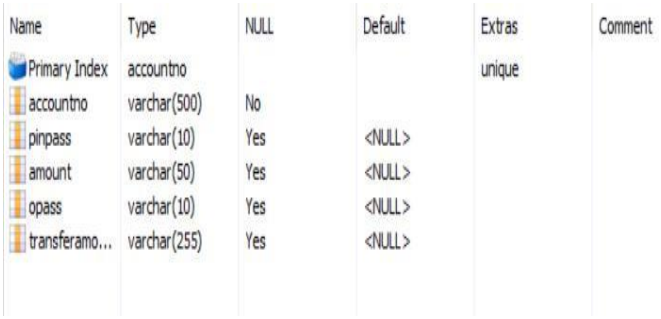
Figure 1 Dataset needed for Traditional level of security in cloud OTP service provider

3.2 Dataset for Secure level of security

Cloud OTP Service Providers provide a good level of security, which is usually used to secure E-Commerce websites. The user's email address, mobile number, and user name and password are the most basic pieces of information required for an E-Commerce website.

Cloud UID also supported multiple factor authentication in addition to the cloud token. Users can browse goods, add products to their cart, and purchase

products they want after completing the registration process in both the cloud platform and the E-Commerce portal. As previously stated, this secure level will provide bank account protection. The cloud will hold a database of the customer's bank account records, including ATM pins and OPass. OPass is nothing more than a ten-bit combination of alphabets and numbers. When a user purchases a product through an E- Commerce site, he or she must have a valid account number, ATM pin, and OPass provided by the cloud.



Name	Type	NULL	Default	Extras	Comment
Primary Index	accountno			unique	
accountno	varchar(500)	No			
pinpass	varchar(10)	Yes	<NULL>		
amount	varchar(50)	Yes	<NULL>		
opass	varchar(10)	Yes	<NULL>		
transferamo...	varchar(255)	Yes	<NULL>		

Figure 2 and Figure 3. Dataset needed for Secure level of security in Cloud OTP service provider and Dataset needed for buying products in E-Commerce website.

3.3 Dataset for Sensitive level of security

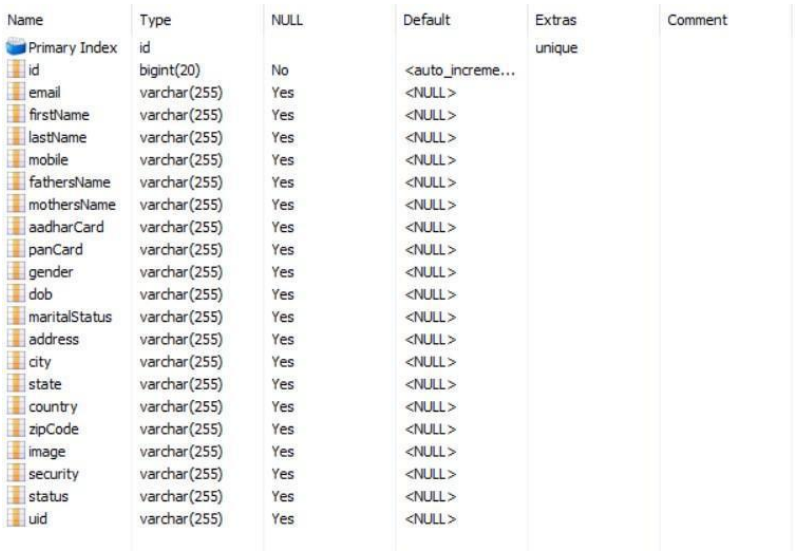
Cloud OTP Service provider takes place in NEFT Bank transaction via Online at this sensitive level of protection. User name, email address, mobile number, Aadhar card number and password are all required fields. The consumer must have an account number and the amount to credit or debit for a NEFT transaction. The user must create an account in both the cloud and

the NEFT Transaction Bank application. Before making a transaction, the user must check his or her account with a smartphone OTP as well as a cloud OTP.

3.4 Dataset for High Sensitive level of security

The Cloud OTP Service provider's High Sensitive level of protection would have access to all other lower security levels. The user's name, email address, mobile number, Aadhar Card, Pan Card number, marital status, and gender are all required at the High Sensitive level. These details are referred to as the customer's KYC information.

This information is obtained from the customer when he or she opens a bank account or a Cloud OTP service account in the cloud. When a transaction occurs in a Bank application, the High Sensitive level of protection will still use Cloud OTP authentication with Cloud Id and Unique ID. Even if outsiders attempt to conduct illegal transactions using mobile OTP, the cloud will never make the transaction because the outsiders do not know the user's cloud Id or UID.



Name	Type	NULL	Default	Extras	Comment
Primary Index	id			unique	
id	bigint(20)	No	<auto_increme...		
email	varchar(255)	Yes	<NULL>		
firstName	varchar(255)	Yes	<NULL>		
lastName	varchar(255)	Yes	<NULL>		
mobile	varchar(255)	Yes	<NULL>		
fathersName	varchar(255)	Yes	<NULL>		
mothersName	varchar(255)	Yes	<NULL>		
aadharCard	varchar(255)	Yes	<NULL>		
panCard	varchar(255)	Yes	<NULL>		
gender	varchar(255)	Yes	<NULL>		
dob	varchar(255)	Yes	<NULL>		
maritalStatus	varchar(255)	Yes	<NULL>		
address	varchar(255)	Yes	<NULL>		
city	varchar(255)	Yes	<NULL>		
state	varchar(255)	Yes	<NULL>		
country	varchar(255)	Yes	<NULL>		
zipCode	varchar(255)	Yes	<NULL>		
image	varchar(255)	Yes	<NULL>		
security	varchar(255)	Yes	<NULL>		
status	varchar(255)	Yes	<NULL>		
uid	varchar(255)	Yes	<NULL>		

Figure 4 Dataset needed for High Sensitive level of security in Cloud OTP service Provider.

Proposed Methodology

Typically, there are four steps in providing Cloud OTP service provider

1. Firstly, the user has to build an account in the cloud platform with required details . The details are checked by the cloud OTP service provider.
2. Secondly, the user have to get a token to his/her registered email Id. And the user have to chose a required level of security provided by the cloud OTP.

3. Thirdly , the user can get the Cloud Id and Unique ID from the cloud OTP . And user have to register themself in chat application , E-Commerce application and Bank application with the same credentials given cloud OTP service provider.
4. Finally , the user are allowed to use the multiple factor authentication in the application registered with Cloud.

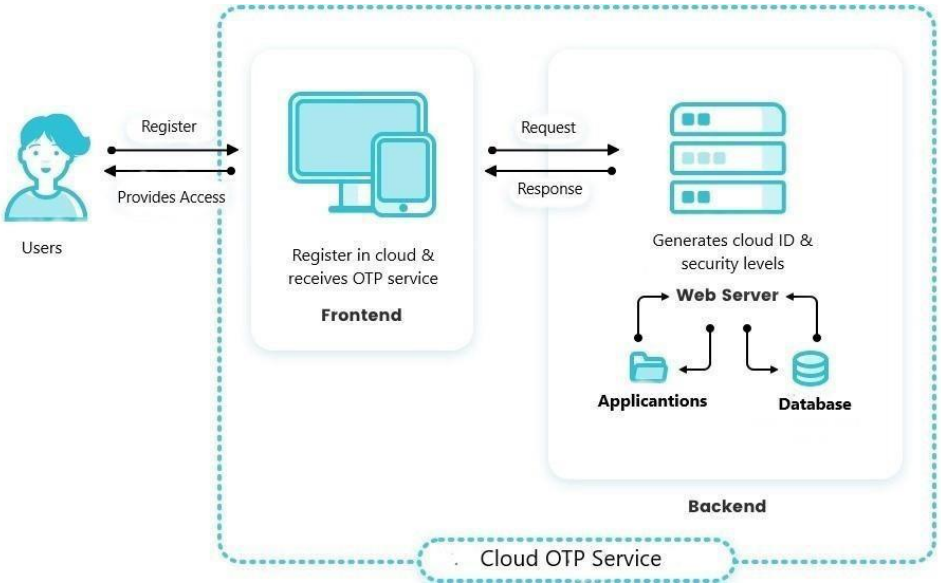


Figure 5 Proposed Diagram of Cloud OTP Service Provider.

4.1 User Registration in Cloud and Choose the Type of security provider

This module allows users to register in the cloud by providing basic information such as their name, email address, and phone number. After registering, the cloud produces a token based on the user's information and sends it to the user's email address. After that, the user must prove his identity by entering the valid token that was sent to his/her email address. If he enters the incorrect token, his/her information will not be saved in the cloud. If the user enters a valid token, he/she will be given the option of choosing between Traditional, Secure, Sensitive, and High Sensitive securities. The user wants to do captcha verification and cloud OTP verification after completing the security selection.

4.2 Verify user details and provide the security in cloud

Cloud owners can receive requests from users with different types of security choices in this module. Cloud owners can check user information and records one by one. If they are unable to locate appropriate documentation and information, they will refuse user requests. If the cloud approves the user request, a unique user ID will be created and sent to the user. Users may be entitled to use certain same requirements applications based on their security settings. He/she is entitled to use all low-level security facilities if he/she has a high security level.

4.3 Traditional OTP as a Service and Bank account creation

In this module, the user needs to build an account in a bank application and add the money to the bank. Every consumer receives an auto-generated account number and ATM pin at that time. If money is sent from the registered account or obtained from another account, the transaction history will be shown. A chat application with traditional authentication can only check the user's mobile number at the time of registration. The traditional cloud OTP service will receive a one-time authentication code from the cloud. By tapping on a specific message in the chat application, we can read our text messages.

4.4 Secure, Sensitive and Highly Sensitive

Grocery store is an e-commerce supermarket application with a secure one- time password (OTP) service. The user can view items, add them to their cart, and delete them from their cart. The quantity of goods in a cart may also be raised or lowered by the consumer. Both secure and traditional features are available in this e- commerce application. It will ask for opt each and every purchase . NEFT Transaction is a secure OTP service that allows you to transfer money to a beneficiary account immediately. There is also the possibility of checking the current account balance. All of the functionality of a secure and traditional OTP service are available with this critical protection. It will prompt the user to choose an option each time he/she logs into his account. An choice called online bank account formation is available in the bank application. For this, the user must send his or her KYC details. If he/she already has a highly sensitive cloud account, he can import all of those data to his bank account by uploading the cloud service and user UID. If he/she provides exact information, the user will receive an OTP. All KYC data will be imported to the bank application after the OTP is completed.

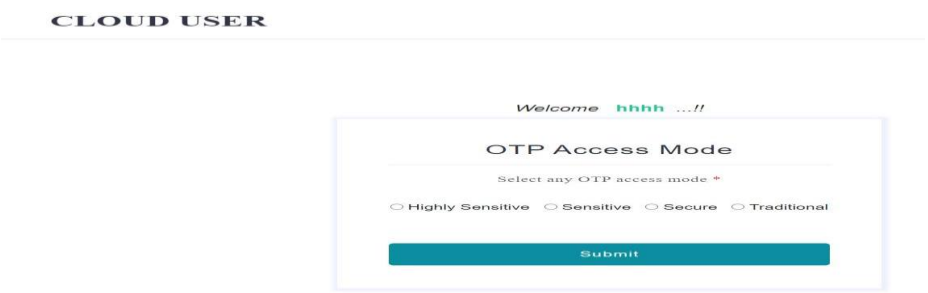
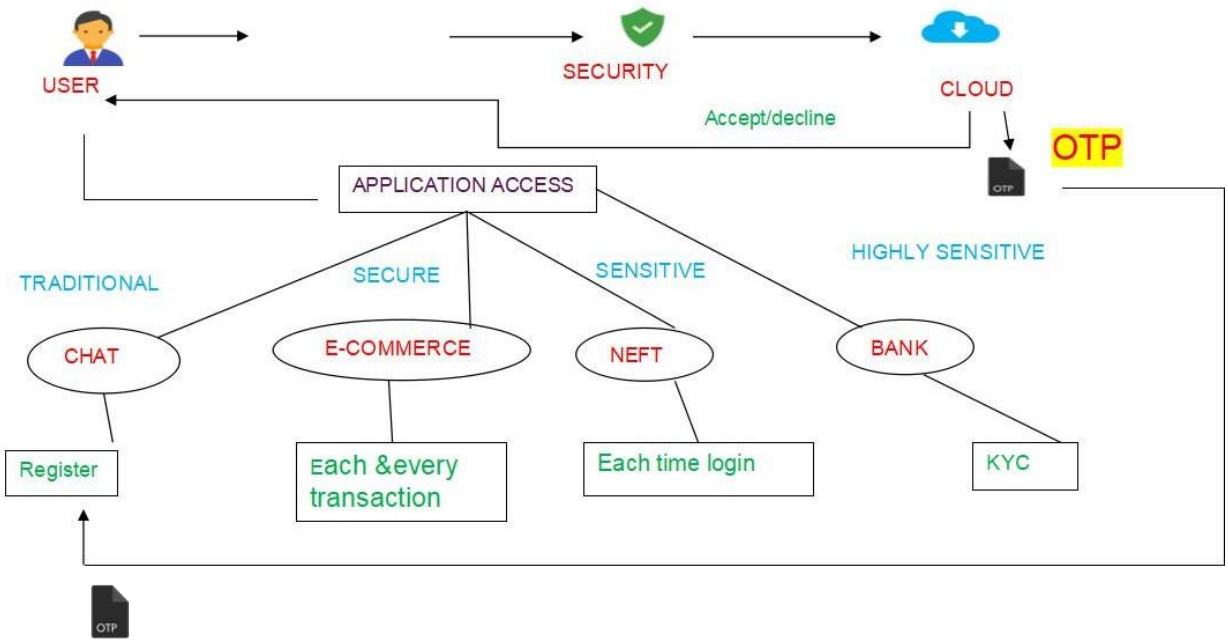


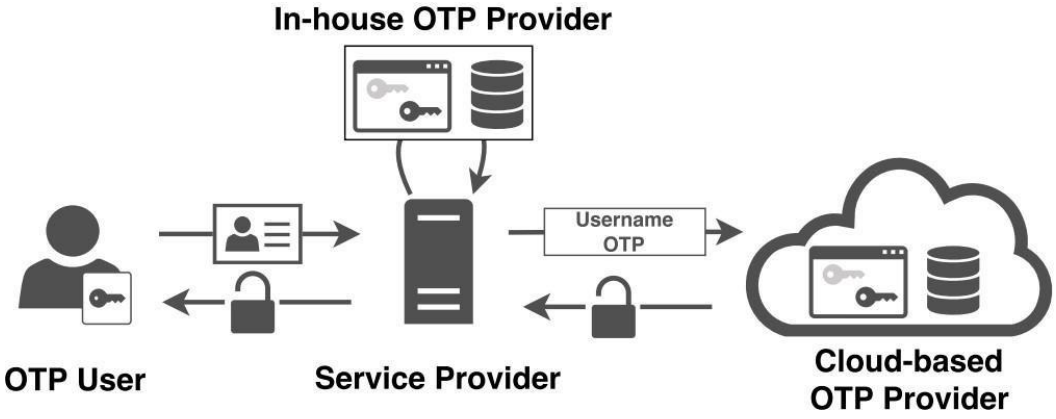
Figure 6 Chose Level of security in Cloud OTP Service Provider

Architecture Diagram

The Architectural Diagram will demonstrate how the proposed system performs. Initially the user must build or set up an account in the cloud platform with the information needed, such as a phone number and email address. After registering on the cloud platform, a cloud token will be generated and sent to the registered email address. Afterwards, it validates the cloud token and requests captcha verification from us. If captcha authentication is performed without any complication and the mobile number is verified as well. If the verification is successful, it will prompt us to pick a cloud OPT service, such as **Traditional** chat applications, **Secure** E-Commerce sites, and S**ensitive** and **Highly Sensitive**

for bank applications with KYC. These four high-priority security services are crucial for data protection and authentication. In order to secure data from outsiders, each degree of protection needs certain information from the user. Individual users are often assigned a unique identifier (UID) in order to provide a high degree of protection. In the Hibernate platform, the phone number and email address are mapped together so that when a user logs into any application with their registered mobile number or email address, the Hibernate platform automatically checks the data in the database. If the information provided is correct, the applicant will be able to access the application; otherwise, it will be denied.





Algorithmic Steps

6.1 RSA ALGORITHM STEPS

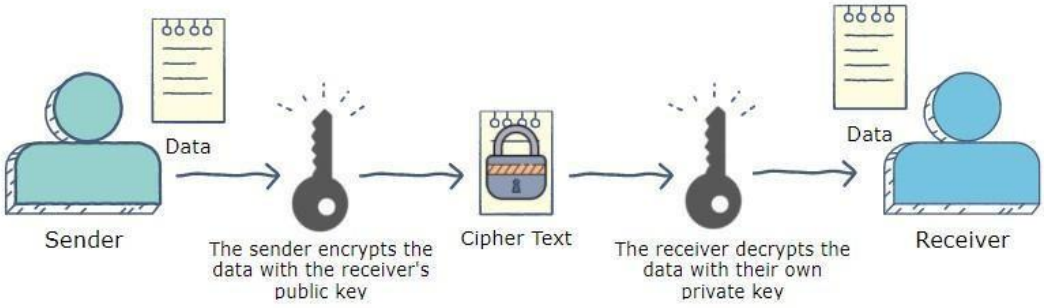


Figure 7 RSA Algorithm for Encryption/Decryption

6.2 Key Generation Algorithm

Step: 1. Choose two very large random prime integers: p and q

Step: 2. Compute n and φ(n):

n = pq and φ(n) = (p-1)(q-1)

Step: 3. Choose an integer e, $1 < e < \varphi(n)$ such that

gcd(e, φ(n)) = 1(where gcd means greatest common denominator)

Step: 4. Compute d, $1 < d < \varphi(n)$ such that: $ed \equiv 1 \pmod{\varphi(n)}$

- the public key is (n, e) and the private key is (n, d)
- the values of p, q and φ(n) are private

- e is the public or encryption exponent

- d is the private or decryption exponent

1) **A simple example for RSA Algorithm**

This is an extremely simple example and would not be secure using primes so small, normally the primes p and q would be much larger.

1. Select the prime integers p=11, q=3.
2. n=pq=33; φ(n)=(p-1)(q-1)=20
3. Choose e=3 Check gcd(3,20)=1
4. Compute d=7 (3)d ≡ 1 (mod 20)

6.3 MD5 (Message-Digest algorithm 5)

MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function that results in a 128-bit hash

value. The 128-bit (16-byte) MD5 hashes (also termed message digests) typically are represented as 32-digit hexadecimal numbers (for example, ec55d3e698d289f2afd663725127bace)

Use of MD5 Algorithm

It was developed with the main motive of security as it takes an input of any size and produces an output if a 128-bit hash value. To be considered cryptographically secure. MD5 should meet two requirements:

1. It is impossible to generate two inputs that cannot produce the same hash function.
2. It is impossible to generate a message having the same hash value.

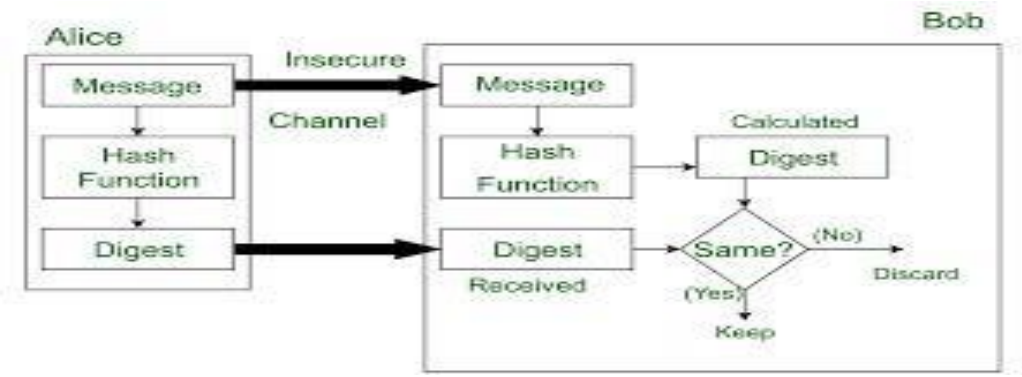


Figure 8 MD5 Algorithm Structure

6.4 How MD5 Algorithm works

Step1: Append Padding Bits: Padding means adding extra bits to the original message.

Step 2: Append Length: After padding, 64 bits are inserted at the end, which is used to record the original input length.

Step 3: Initialize MD5 buffer: A four- word buffer (A, B, C, D) is used to compute the values for the message digest.

Result and Observation

Cloud OTP as a service is used to incorporate the proposed framework. The

Cloud OTP service also includes four levels of protection in all of its applications, resulting in a safe environment for users to communicate and move money. The proposed system also lowers the cost for developers to generate OTP for their applications. Multiple factor authentication can be achieved by combining Cloud Token with Cloud OTP and Captcha verification. As previously mentioned, there is a very slim risk of an outsider targeting the website.

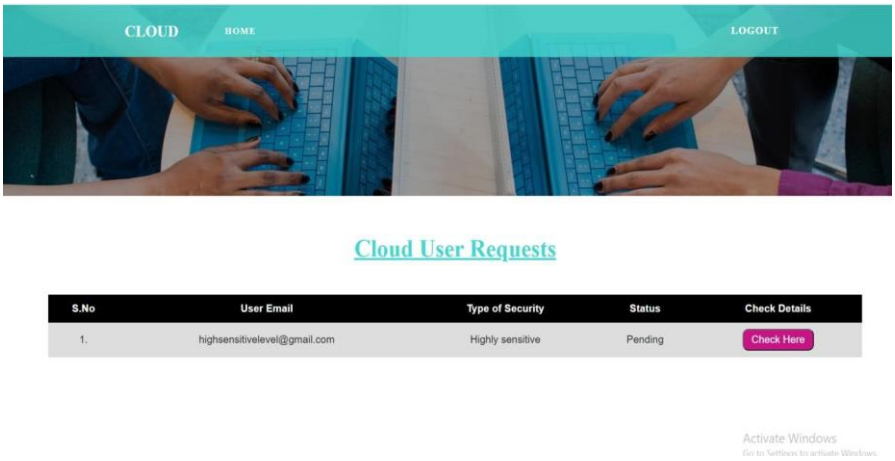


Figure 9 High Sensitive level in Cloud OTP Service Provider

Conclusion and Discussion

To summarise the proposed system, the features included here outperform the current process. With powerful technological advancements, the proposed system would be able to adapt to changes in the protection level offered by any application. Multiple factor authentication takes the place of two-factor authentication in such a way that fraudsters are never able to gain access to the user's account. Currently, the protection level is limited to a few applications, although this type of functionality will be enhanced in the future..

References

[1] Prototype model for enhancing security of one time password otp in ebanking using encrypted unicode sms eusms technique - Nov 2017.
[2] Algorithms for Enhancing Intelligence Based Service Level Agreement Towards Secured Cloud Environment - Oct 2016.
[3] Secured SMS Receiver System for Android Devices Sep 2020.

[4] Secure Human Healthcare Monitoring Mechanisms in Wireless Body Area Networks - Apr 2020.
[5] Web application characterization and evaluation using a black box model - May 2016.
[6] Lightweight Algorithms for Data Security in Healthcare Internet of Things - Apr 2020.
[7] A New Graphical Password: Combination of Recall & Recognition Based Approach",Md. Asraful Haque, Babbar , 2014.
[8] AntiPhishingGroup, "Phishing Activity Trends Report", Dec 2008.
[9] Sang-Il Cho, HoonJae Lee, Hyo-Taek Lim, Sang-Gon Lee, "OTP Authentication Protocol Using Stream Cipher with Clock- Counter",October, 2009.
[10] Jean-Daniel Aussel, "Smart Cards and Digital Identity", 2007.
[11] An HMAC-Based One-Time Password Algorithm, Dec. 2005.
[12] International Symbology Specification – Data Matrix, 2000.
[13] Automatic Identification and Data Capture Techniques – BarCode Symbology – QR Code, 2000.
[14] Barcode Readers using the Camera Device in Mobile Phones, Conference on Cyber worlds, pp.260-265, 2004.
[15] Reilly, D., Smolyn, G. and Chen, H., "Toward fluid, mobile and ubiquitous interaction with paper using recursive 2D barcodes", 2007.
[16] Evaluating authentication mechanisms , L. Cranor and S. Garnkel,2005.
[17] A large-scale study of WWW password habits , D. Florencio and C. Herley , May 2007.
[18] Authenticating Mobile Device Users Through Image Selection, in Data Security,W. A. Jansen ,2004.
[19] Designing Graphical Authentication for Security" Martin Mihajlov E,2011.
[20] Design and Analysis of a Graphical Password Scheme", International , Haichang Gao, Xiyang Liu, Ruyi Dai, 2009 .
[21] Lightweight Authentication Method , Christopher Varenhorst July 2004.
[22] Mohammad Mannan, P. C. Van Oorschot, "Security and Usability: The Gap in Real-World Online Banking, Sep. 18-21, 2007