Secure Authentication Scheme using mobile-otp generation

[1]S.Varsha, [2]D.Swapna, [3]N.Mounika, [4]V.Supraja
[1]Student, [2]Associate Professor, [3]Student, [4]Student
BVRIT Hyderabad College Of Engineering For Women

Abstract - **Authentication performs the main function in securing any online banking systems and services that have long relied on username/password mixtures to verify customers. Memorizing usernames and passwords for a variety of systems becomes an inefficient task. Legacy authentication strategies have failed again and again, and they may be not immune in opposition to a huge kind of attack. Over the years, records emphasize that attackers have created numerous high-tech techniques to steal user's credentials that may pose a serious hazard. In this paper, we recommend a green and practical person authentication scheme with the use of private devices that utilize distinctive cryptographic primitives. Our proposed system does no longer require an authentication server to keep the static username and password tables for figuring out and verifying the legitimacy of the login users. It is comfortable against password associated attacks, however, it can also resist replay attacks, and shoulder browsing attacks, phishing attacks, and records breach incidents.**

keywords **- Authentication, Online banking system, Legacy authentication, attacks, private devices, replay attacks, phishing attacks.**

I. INTRODUCTION

"Secure Authentication Scheme using mobile-otp generation" is an application that provides a secure procedure for login for banking purpose. Mobile is a necessary commodity for all the human beings in this contemporary world. Using the mobile phone we can provide more authentication for banking purpose login. As there are many security threats like Phishing Attacks, Password-Related Attacks, Replay Attacks…etc. These kind of security threats can leads to disruptions in the login process securely. To provide security from these attacks, this system enables us to prevent security threats to some extent. To achieve authentication the application registers the user's email id to send the credentials. Using the security algorithms like Elliptic Curve Digital Signature Algorithm (ECDSA) and Advanced Encryption Standard (AES), the OTP is generated. The user of the application can request for one time username and password. The system will be able to send the requested details to the user registered email. This system enables the user complete protection to the user without the burden of remembering the username and password.

II. EXISTING SYSTEM

The traditional system that exists currently enables the system to generate OTP for banking transaction. It is also observed that is convention for all the user to remember all the usernames and passwords. Studies says that all the usernames and passwords are similar for the accounts, so it can make them vulnerable to attacks. The proposed system enables us to eliminate the all the risks encountered in the existing system.

Limitations of Existing System

- Prone to forget credentials
- Liable to hacks
- Burden to remember credentials
- Easy to decrypt using less protected algorithms

All the above drawbacks are overcome in the proposed system.

III. PROPOSED SYSTEM

The proposed system is flexible for the user. The user does not have the burden to remember all the username and the password. The username and the password are generated on the request of the user. The username and the password are sent to the registered email. The user can then enter the username and password in the necessary fields. This can be one of the model for securing our personal information. This design considers the principle of giving a user account only those privileges that are essential to that user's work.

IV. ARCHITECTURE

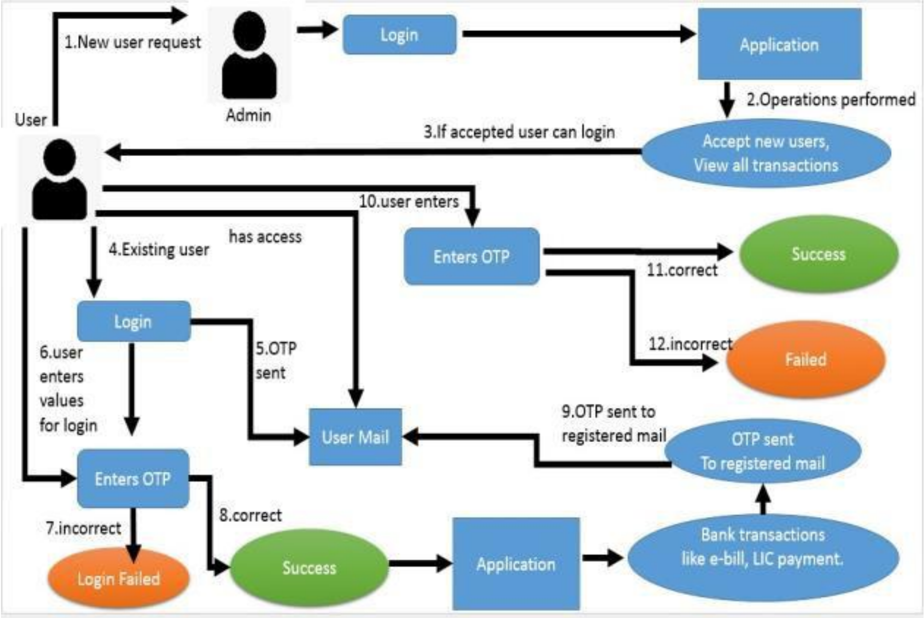


Fig.1 System architecture

V. IMPLEMENTATION

The procedure starts with the user registering in the application. The admin had the authority to accept or decline the user's request. After the acceptance of the user's registration, the user can perform respective transactions according to their will like LIC payments, pay all basic necessities bill, and transfer money to others. The admin can view all the transactions made by all the users.

Modules:

This project having the following modules:

- User
- Admin

User:

In this project, the user is allowed to transfer the money from his/her account to another through this site. For this purpose, the user needs to request admin to activate the account. After activating the account, the user is allowed to request for the OTU and OTP. After getting OTU and OTP the user can login into the site with their credentials (OTU and OTP) and can perform the transactions. If user is idle after logging in without performing any operation, within a particular session time (10 minutes), the user is logged out automatically. For each transaction the user gets OTP to his personal device. Using that OTP user can complete his/her transaction.

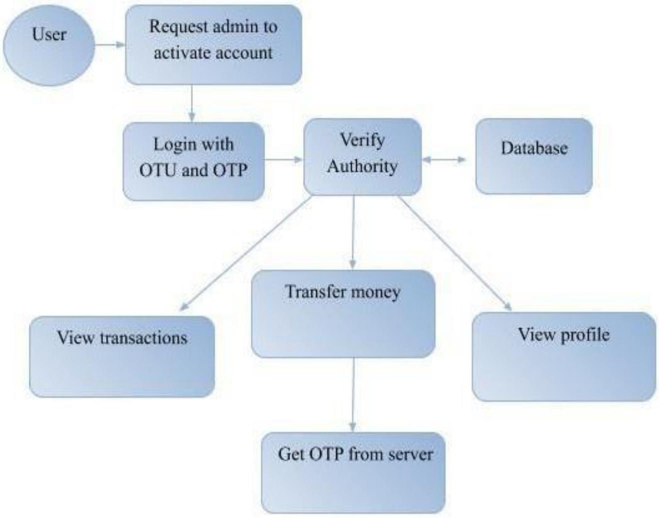


Fig.2 User module diagram

Admin:

In this project, the admin is allowed to activate the user account by accepting the request sent by the user. He can also view transactions like Tax Payment, E-Seva Transactions, Credit card bill Payment, LIC Transactions performed by users.

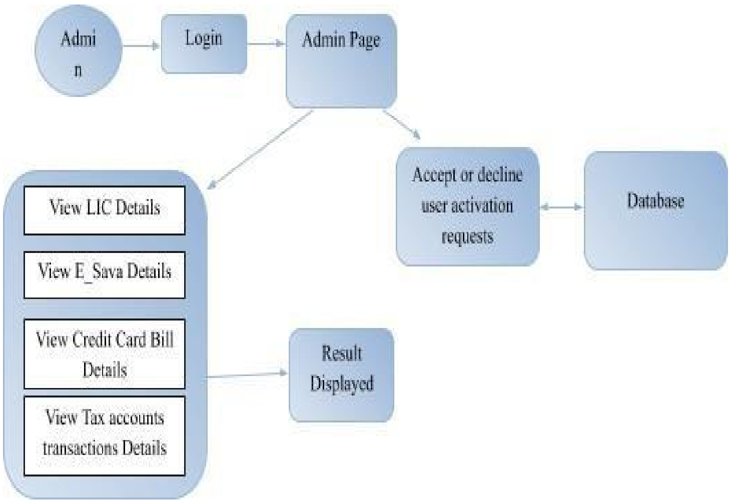

Admi
n
Login
Admin Page
Accept or decline user activation requests
Database
View LIC Details
View E_Sava Details
View Credit Card Bill Details
View Tax accounts transactions Details
Result Displayed

Fig.3 Admin module diagram

Algorithms:

To provide security to the application following algorithms are used. The algorithms used in the application are

- Elliptic Curve Digital Signature Algorithm (ECDSA)
- Advanced Encryption Standard (AES)

ECDSA Algorithm:

Elliptic Curve Digital Signature Algorithm or **ECDSA** is a cryptographic algorithm used by Bit coin to ensure that funds can only be spent by their rightful owners. Elliptic Curve Digital Signature Algorithm (ECDSA) which is one of the variants of Elliptic Curve Cryptography (ECC) proposed as an alternative to established public-key systems such as Digital Signature Algorithm (DSA) and Rivest Shamir Adleman (RSA), have recently gained a lot of attention in industry and academia. The keys generated by the implemented software is highly secured and it consumes lesser bandwidth because of small key size used by elliptic curves and this is also coupled with the introduction of open source software into this work, which is generally believed to be more secured than those traditionally available on closed source operating systems like Microsoft Windows. Significantly smaller parameters can be used in ECDSA than in other competitive systems such as RSA and DSA, but with equivalent levels of security. Some benefits of having smaller key sizes include faster computation time and reduction in processing power, storage space and bandwidth. These advantages are especially important in other environments where processing power, storage space, bandwidth, or power consumption are lacking.

Before starting the protocol, a user should specify two parameters:

1. We introduce the concept of user-centric access control, which can play a pivotal role in authentication and enhance security. In user-centric access control, users are in charge, and they can set their account permission for each login session. (e.g. passive mode or active mode)
2. The ticket validity period TVP (e.g. 5 minutes).The following describe the complete protocol for requesting a ticket and verifying a user by the server. The registered device generates a ticket M with the following information. A randomly generated one-time username OTU, the required permission ACL, and the specified ticket validity period TVP M=OTU||TVP||ACL

AES algorithm:

This algorithm is used to provide confidentiality to the user credentials. The Advanced Encryption Standard, or AES, is a symmetric block cipher which is used as a specification for the encryption of electronic data.

How AES encryption works

AES comprises three block ciphers: AES-128, AES- 192 and AES-256.AES-128 uses a 128-bit key length to encrypt/decrypt a block of messages, AES-192 uses a 192- bit key length and AES-256 a 256-bit key length to encrypt/decrypt messages. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256- bits, respectively. Symmetric (also known as secret-key) ciphers use the same key for encrypting and decrypting, so the sender and the receiver must both know and use the same secret key.

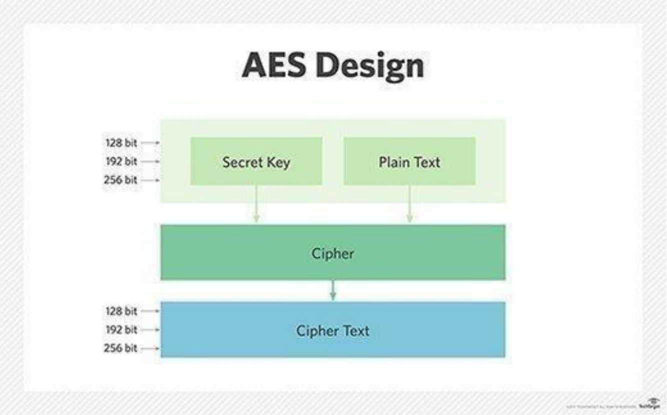
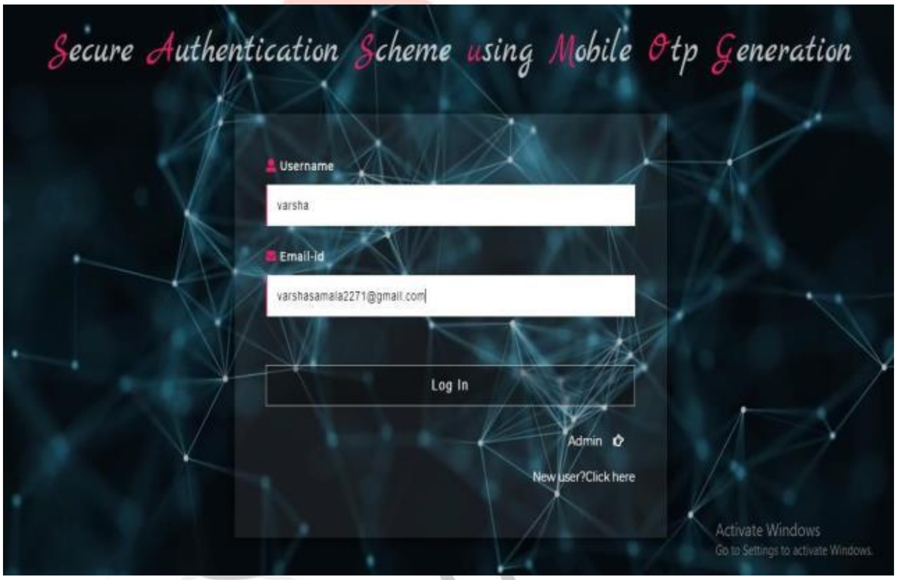


Fig.4 AES Design

The AES encryption algorithm defines a number of transformations that are to be performed on data stored in an array. The first step of the cipher is to put the data into an array; after which, the cipher transformations are repeated over a number of Encryption rounds. The number of rounds is determined by the key length, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

RESULT

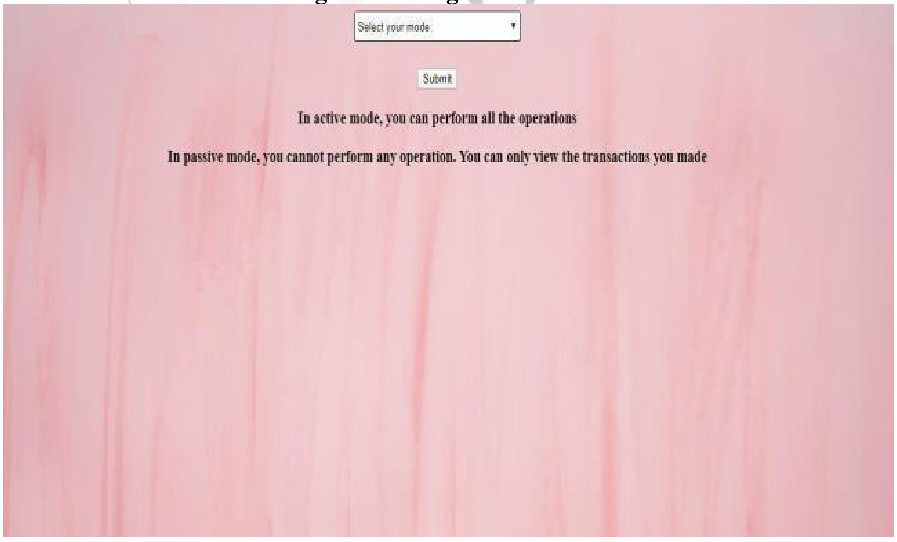

Secure Authentication Scheme using Mobile Otp Generation

Username: varsha

Email-id: varshasamala2271@gmail.com

Log In
Admin
New user?Click here
Activate Windows
Go to Settings to activate Windows.

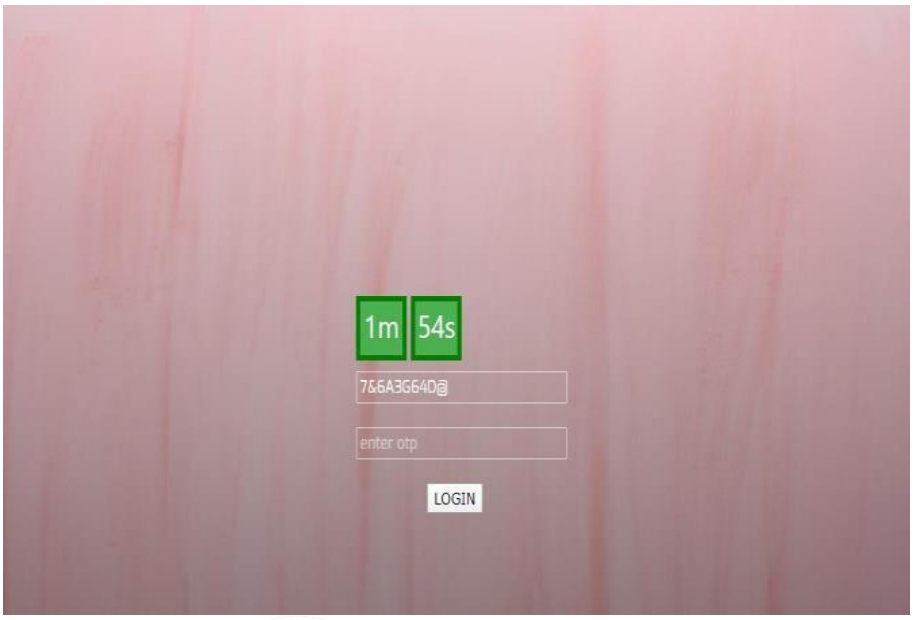
Fig.5 User Login Form



In active mode, you can perform all the operations

In passive mode, you cannot perform any operation. You can only view the transactions you made

Fig. 6 Selection of Access Control Mode

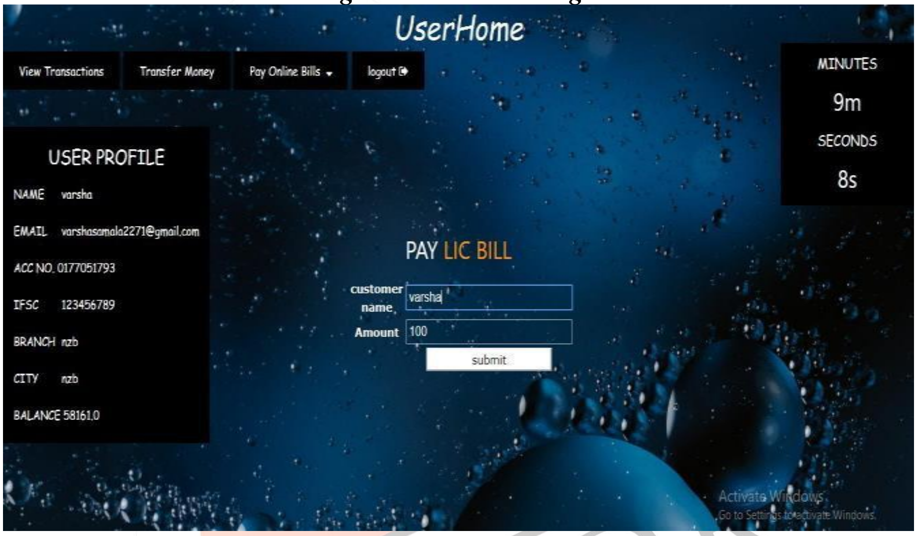


1m 54s

7&6A3G64D@

enter otp

Fig. 7. Enter OTP to login



UserHome

MINUTES
9m
SECONDS
8s

USER PROFILE

NAME varsha

EMAIL varshasamala2271@gmail.com

ACC NO. 0177051793

IFSC 123456789

BRANCH nzb

CITY nzb

BALANCE 58161.0

PAY LIC BILL

customer name varsha

Amount 100

Fig. 8. Bill payment page

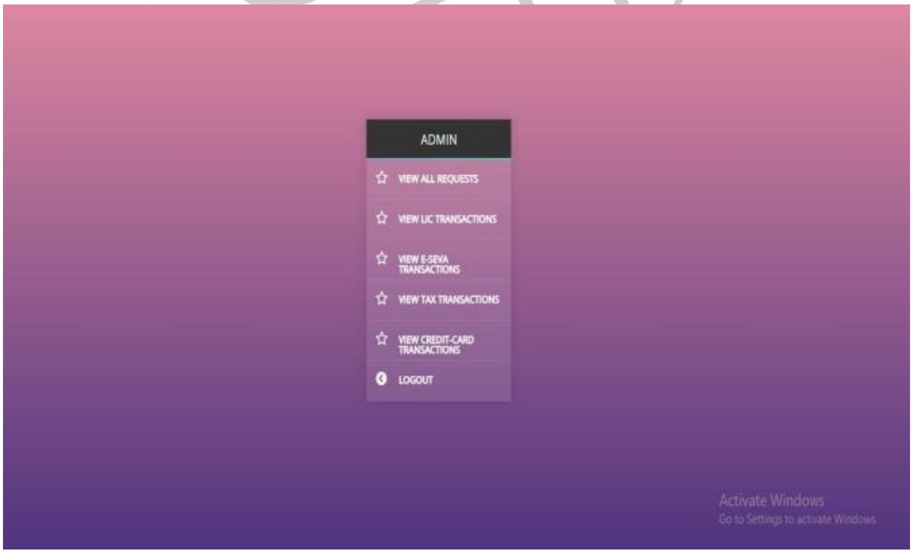
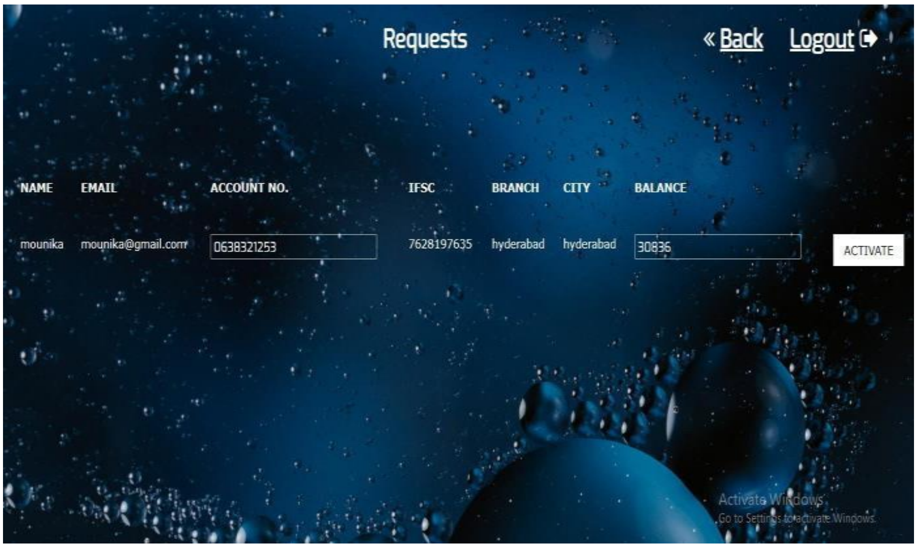
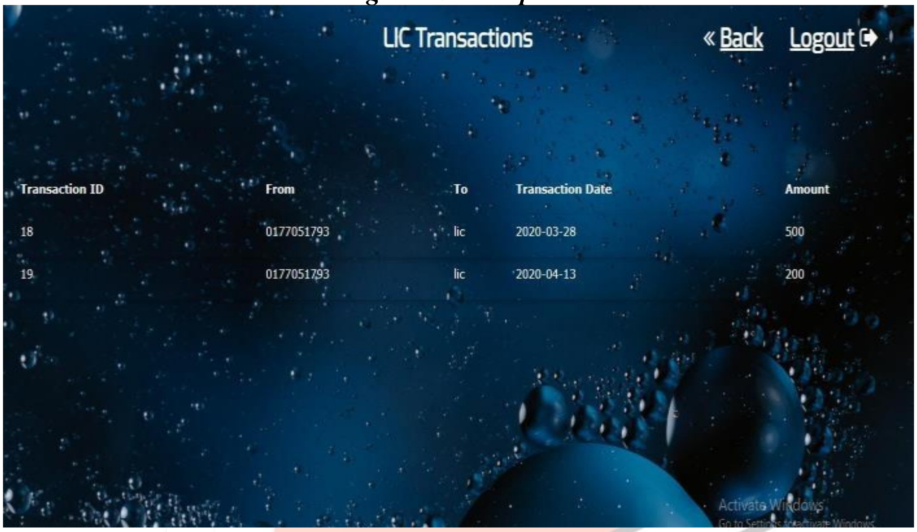


Fig. 9. Admin Home page



NAME	EMAIL	ACCOUNT NO.	IFSC	BRANCH	CITY	BALANCE
mounika	mounika@gmail.com	0638321253	7628197635	hyderabad	hyderabad	30836

Fig. 10. User request



Transaction ID	From	To	Transaction Date	Amount
18	0177051793	lic	2020-03-28	500
19	0177051793	lic	2020-04-13	200

Fig. 11. Transaction history of all users

VI. CONCLUSION

In the digital world, any kind of work can be done on the computer. To provide security to all those online works this application can be used.

For all banking transactions and e-commerce websites it can appropriate to use. Using the latest algorithms high security is provided. The username and the password are unique and cannot be easily decoded

VII. REFERENCES

[1] A. Alhothaily, A. Alrawais, X. Cheng, and R. Bie. A novel verification method for payment card systems. Personal and Ubiquitous Computing, 19(7):1145–1156, 2015.

[2] A. Alrawais, A. Alhothaily, C. Hu, X. Xing, and X. Cheng. An attribute based encryption scheme to secure fog communications. IEEE Access, 2017.

[3] K. Aravindhan and R. Karthiga. One time password: A survey. International Journal of Emerging Trends in Engineering and Development, 1(3):613–623, 2013.

[4] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In Security and Privacy (SP), 2012 IEEE Symposium on, pages 553–567. IEEE, 2012.

[5] Google 2-step verification. Available at http://www.google.com/2step, Date last accessed 2-Feb-2016.

[6] A. Hiltgen, T. Kramp, and T. Weigold. Secure internet banking authentication. IEEE Security Privacy, 4(2):21–29, March 2006.

[7] Y. S. Lee, N. H. Kim, H. Lim, H. Jo, and H. J. Lee. Online banking authentication system using mobile-otp with qr-code. In Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on, pages 644–648. IEEE, 2010.

[8] Java timer available at https://www.oracle.com/technicalresources/articles/java/java- timers.html

[9] Java OTP generation available at https://www. codespeedy.com/otp-generation-in-java/