Brightness Based Password Authentication to Avoid Shoulder Surfing in Banking Applications

Author

Dr.R.Kanimozhi[1],D.Swetha[2],S.kowsalya[3],J.Nasrath Banu[4],R.Sowmiya[5]

A.V.C College of Engineering& IT& Anna University& Mayiladuthurai, Tamil Nadu

1.Dr.R.Kanimozhi,Ph.D.,Assisstant Professor ,A.V.C College Of Engineering, Mayiladuthurai.
2.D.Swetha,IV Year, B.Tech(IT),A.V.C College Of Engineering, Mayiladuthurai.
3.S.Kowsalya, IV Year, B.Tech(IT),A.V.C College Of Engineering, Mayiladuthurai.
4.J.Nasrath Banu, IV Year, B.Tech(IT),A.V.C College Of Engineering, Mayiladuthurai.
5.R.Sowmiya, IV Year, B.Tech(IT),A.V.C College Of Engineering, Mayiladuthurai.

ABSTRACT:

This project deals with problems on providing security Bright Pass is a user authentication scheme for secure ATM application. Shoulder surfing refers to eavesdropping one's personal information like PIN or passwords by observing it from a considerable distance. we address this issue by introducing Bright Pass, a novel authentication mechanism based on screen brightness. Bright Pass allows users to authenticate safely with a PIN-based confirmation in the presence of specific operations on sensitive data. In this approach user can enter their PIN regarding the brightness value displayed to the user.

KEYWORDS: Malware, Brightness, Usability, novel authentication.

INTRODUCTION:

PIN authentication is very common in ATM process. Intruders can break this PINs using shoulder surfing or guessing methods. Bright pass allows user to authenticate safely with a PIN-based confirmation in the presence of specific operations on sensitive data. To avoid attacks in ATM process provides brightness based pin authentication. The user details are stored in ATM server database. User should login with username and PIN. While entering the PIN, the normal keypad will be changed to a bright pass based keypad. After each login, the keypad will be shuffled. This is done to avoid shoulder surfing.

EXISTING SYSTEM:

Net banking is one of the important applications to make transaction easy through user mobile phone. User authentication is important to verify whether the user is valid or not.PIN is a method to verify user based on sequence of numbers.

Proposed system:

To overcome password guessing and shoulder surfing attacks. we are using for OTP for each transaction and including shuffling.

LITERATURE REVIEW:

A).A Survey of password attacks and comparative analysis on Methods for secure authentication:

It involves real and unique signature and it cannot be stolen. But it is costly and difficult.

B). Fake Pin: Dummy key based mobile user Authentication scheme

To assured good usability as well as to prevent shoulder surfing, guessing and smudge attacks. But it is still not mature and can be by passed.

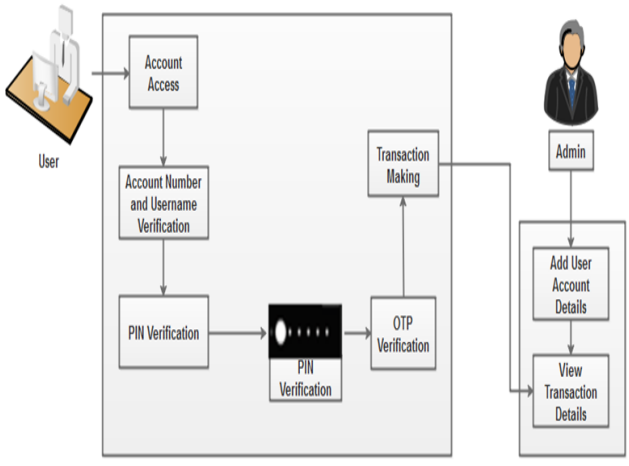

Fig.1: SystemArchitecture

MODULES:

FRAMEWORK CONSTRUCTION

Admin has to register the appropriate details in the server database for ATM template. These details are stored in the first server database. User should login with username and PIN. While entering the PIN, the normal keypad will be changed to a Bright pass based keypad. If

the details entered matches with the details available, the user will be redirected to the home page. After each login, the keypad will be shuffled. This is done to avoid shoulder surfing.

USER AUTHENTICATION

Anonymous access is the most web site access control method, which allows anyone visit the public areas of a websites while preventing unauthorized users from gaining access to critical features and private information of web service. The user verification phase analyze the user name, password to the ATM server. The second stage verifies the Bright pass based password for PIN verification. Both verification gives the permission to access the online bank template and then changes the second password value.

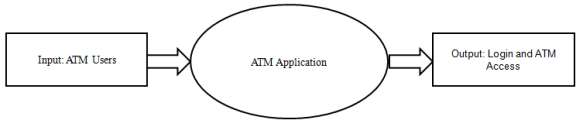

Fig.2:User Login

BRIGHT PASS SYSTEM

Bright pass is designed to protect PIN code from automatic action/operation approval by malware. In Bright pass authentication session, where the user inputs PIN and lie digits according to the circle's brightness. A bright circle tells the user to input a correct PIN digit(highlighted in green)while a dim circle means to enter a missing lie digit(highlighted in red).Here used gray colour to show the dim circle for presentation purpose, since the screenshot cannot capture the device's brightness.

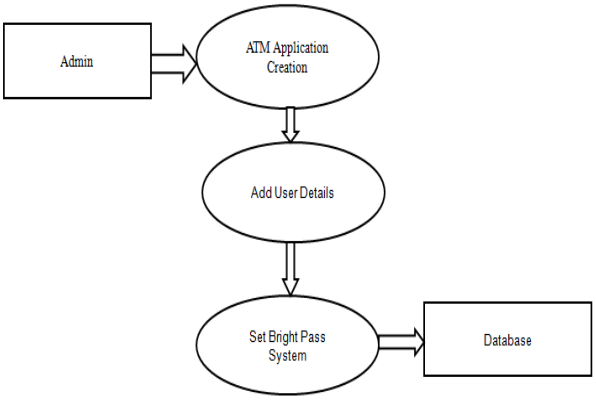

Fig.3:ATM Application Creation

ATM APPLICATION

To get access to purposed ATM facility, a admin would need to register with the institution for the provider, and set up a password and different credentials for user verification. User shoulder complete the verification criteria the access ATM application. In ATM application, user can perform transaction, withdrawal, balanced enquiry and mini statement details.

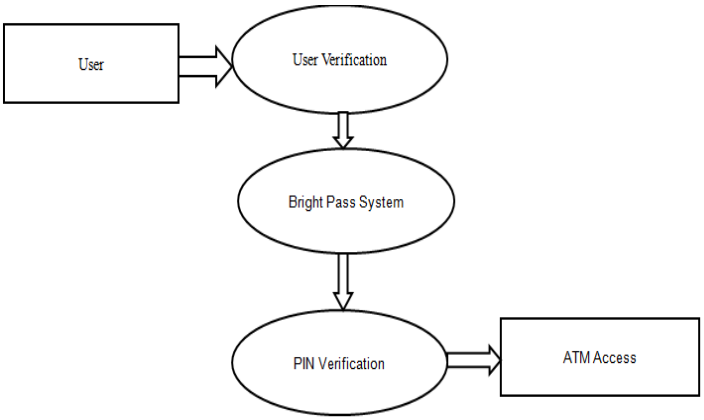

Fig.4:Accessing Operation

ALGORITHM:

AES ALGORITHM:

This algorithm begins with and add round key stages followed by 9 rounds of 4 stages and a 10^{th} round of 3 stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of its counterpart in the encryption algorithm.

ENCRYPTION:

_substitute bytes
_shift rows
_mix columns
_add round key

The tenth round simply leaves at the mix column stage.

DECRYPTION:

The first nine rounds of decryption algorithm consists of following:

_inverse substitute bytes
_inverse shift rows
_inverse mix columns
_inverse add round key.

Again the tenth round simply leaves out the inverse mix columns stage.

CONCLUSION

A project of authentication method(Bright pass) that prevents malware from able to compromise net banking and subvert user authenticated operation. The proposed scheme uses screen brightness as a secure communication channel to communicate a random sequence generated by secure element to user. Thus, the user authenticates with a new trial for each authentication. The security analysis shows the proposed scheme is resilient against brute force attacks, dictionary attacks, side channel attacks and spyware based recording attack.

REFERENCES

[1] Caviglion,L.,Cocoli,M.,Merlo,A.:A taxonomy-based model of security and privacy in online social networks(2014) International Journal of Computational Science and Engineering,9 (4),pp.325-338.DOI: 10:1504/IJCSE.2014.060717

[2] Ikhalia,E.,Imafidon,C. O.: Then need for two factor authentication in social media. In Processing's of the International Conference on future Trends in computing and Communication-FTC,(2013)

[3] Kim,H., Tang,J.,Anderson,R.Social authentication: harder than it looks.In Financial Cryptography and Data Security,pp. 1-15 Springer Berlin Heidelbrg,(2013).

[4] Aviv, A. J., Sapp,B., Blaze, M., smith, J. M.: Practicality of accerlerometer slide channels on smart phones.In ACSAC'12:proceedings of the 28th Annual Computer Security Applications Conference,pp. 41-50. ACM, New York,NY,USA(2012). Doi:10.1145/2420950.2420957.

[5] Simon,L., Anderson,R., PIN Skimmer.Infering PINs Through The Camera and Microphone.In SPSM 13: Proceedings of the Third ACM Workshop on Security and Privacy in Smartphone's and Mobile devices,pp. 67-78. ACM New York,Ny,USA(2013).Doi:10.1145/251676.02516770.