Synopsis

Title: E-Authentication System

Project Member: Ku. Rashmita Rajendra Wade

ABSTRACT

Authenticating the students' identity and authenticity of their work is increasingly important to reduce academic malpractices and for quality assurance purposes in Education. There is a growing body of research about technological innovations to combat cheating and plagiarism. However, the literature is very limited on the impact of e-authentication systems across distinctive end-users because it is not a widespread practice at the moment. A considerable gap is to understand whether the use of e-authentication systems would increase trust on e-assessment, and to extend, whether students' acceptance would vary across gender, age and previous experiences. This study aims to shed light on this area by examining the attitudes and experiences of 328 students who used an authentication system known as adaptive trust-based e-assessment system for learning (TeSLA). Evidence from mixed-method analysis suggests a broadly positive acceptance of these e-authentication technologies by distance education students. However, significant differences in the students' responses indicated, for instance, that men were less concerned about providing personal data than women; middle-aged participants were more aware of the nuances of cheating and plagiarism; while younger students were more likely to reject e-authentication, considerably due to data privacy and security and students with disabilities due to concerns about their special needs.

OVERVIEW

Authentication is a process to access to login account and accessing the service provided by the system or server using the password. It also has an alternative way to authenticate the user which is using biometric authentication by using fingerprint or iris recognition. However, human has the tendency to create easily remember password which it will lead to a problem. By definition, authentication is the use of one or more mechanisms to confirm that you are the authenticated user. Once the identity of the human or machine is validated, access is granted. There are existing acknowledged three authentication factors are things the user knows, things the user have and biometric authentication. Biometric-based

authentication is a good way to authenticate the user but it is expensive and raises some privacy concern. One Time Passwords (OTP) offers a promising alternative for two-factor authentication systems. A one-time password is a password that is valid for only one login session or transaction, on a computer system or other digital device (Cheng, X. R. et al. ,2005). Two-factor authentication solution equips customers with a cost-effective means of providing flexible and strong authentication to very large scale. The goal of computer security to maintain the integrity, availability and privacy of the information entrusted to the system can be obtained by adopting this authentication technique.

PURPOSE

Electronic authentication is the process of establishing confidence in user identities electronically presented to an information system.[1] Digital authentication, or e-authentication, may be used synonymously when referring to the authentication process that confirms or certifies a person's identity and works. When used in conjunction with an electronic signature, it can provide evidence of whether data received has been tampered with after being signed by its original sender. Electronic authentication can reduce the risk of fraud and identity theft by verifying that a person is who they say they are when performing transactions online.

SCOPE

The scope of National e-Authentication is limited to the delivery of all government services through internet/mobile. The intention of National e-Authentication is to assist all government departments/agencies at both central and state levels in the selection and implementation of appropriate authentication mechanisms for delivery of government services through internet/mobile.

PROPOSED SYSTEM

The user can easily and efficiently login into the system. We analyze the security and usability of the proposed scheme, and show the resistance of the proposed scheme to hacking of login credentials, shoulder surfing and accidental login. The shoulder surfing attack can be performed by the adversary to obtain the user’s password by watching over the user’s shoulder as he enters his password. Since, we have come up with a secure system schemes with different degrees of resistance to shoulder surfing have been proposed. In order to use this authentication system, user need to first register himself into this system by filing up the

basic registration details. After a successful registration, user can access the login module where he/she need to first authenticate the account by entering the email id and password which was entered while
registration.

Draft National e-Authentication Framework (NeAF)

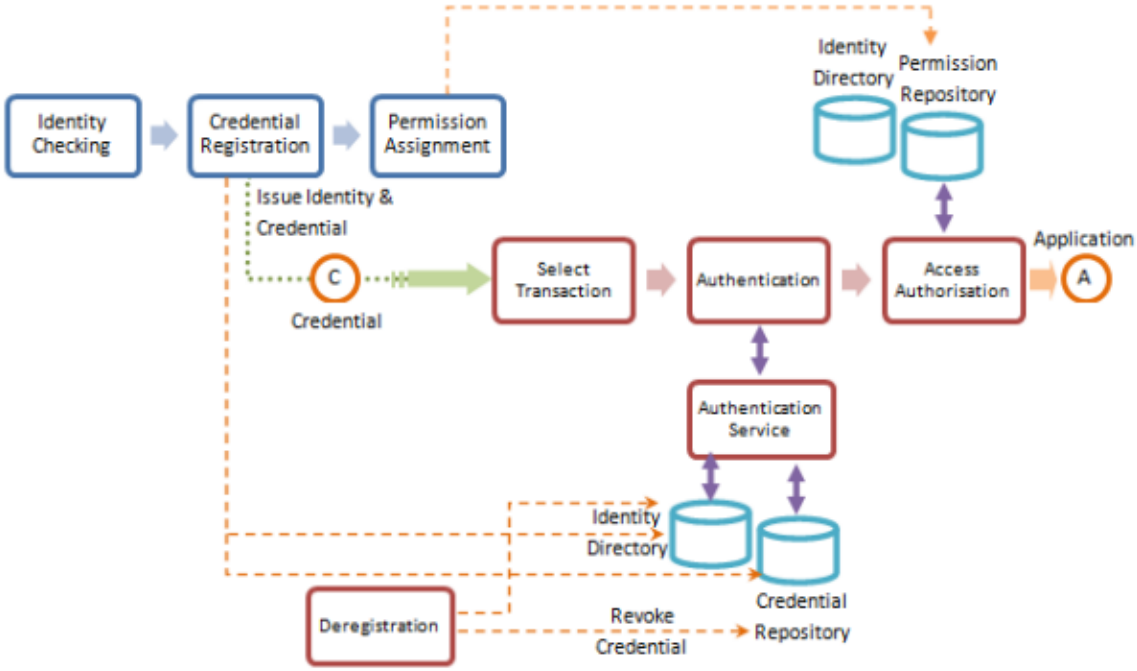
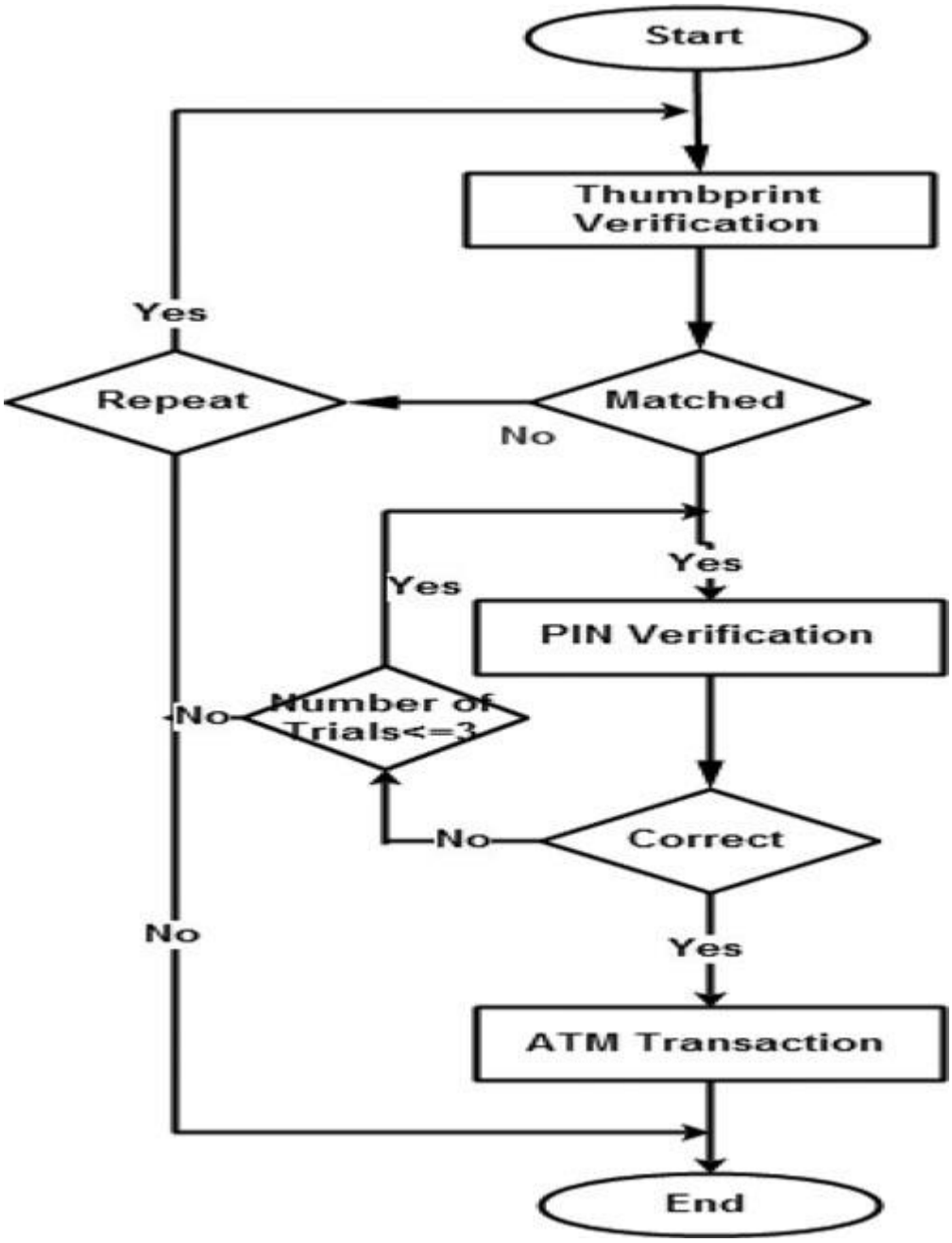


Figure 3-1 - Identity and Access Management

Once the email id and password are authenticated, the user may proceed with next authentication section where he/she need to select the type of authentication as QR (Quick Response) Code or OTP (One Time Password). Once the user selects the authentication type as QR Code, then system will generate a QR Code and send it to user's mail id over internet. If user select's OTP, then SMS will be sent on his/her registered mobile number. If the user passes the authentication, then system will redirect to the main page. The QR Code and OTP

are randomly generated by the system at the time of login.



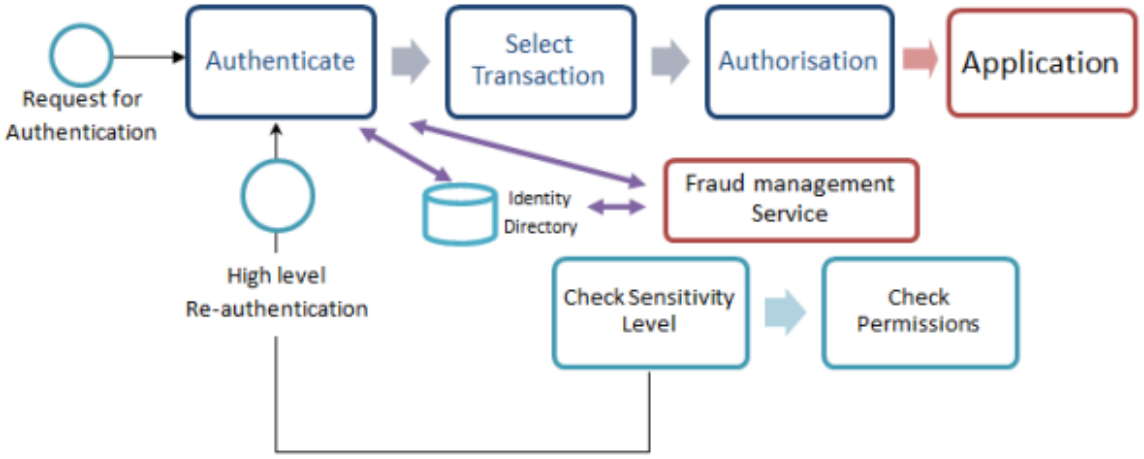


Figure 2-1 Process Flow

SYSTEM REQUIREMENT

Software Requirement:

Advanced Authentication Appliance runs 64-bit operating system on x86-64 .

Hardware Requirement :

Hardware supported by SLES 12 SP4.

OBJECTIVE

1. The main objective is to implement a secure login authentication system with utilizing with two-factor authentications. By using the concept two-factor authentication could help to increase the strength of the login system. The attacker will need to pass through the next barrier of defence to success to log in. This system will help to enhance the login authentication system.

2. Next objective is to ensure login password will not be transmitted over the network. As compared to the previous solution, the password is just encrypted, but the attackers might succeed to decode the data and retrieve the password. So, in order to prevent this happens, the password with the random key will need to be hash before the sender sends the password to the server. It is important to secure the password of the user.

3. Apart from that, the third objective will be to generate the one-time password offline. This will help in perform the login procedure if there is a limited connection of wi-fi or mobile signal is weak. It will help the user who lives in the countryside which has a weak phone signal.

4. Lastly, the fourth objective is to ensure the system is protected from rainbow table attack. The rainbow table will act as a dictionary store and optimised for hashes and password. So once the random key is repeated, the password will be retrieved. So, the random key should be long enough to cause the attackers to use a longer time to generate the rainbow table.

CONCLUSION

From what we have discussed in this video , authentication very important for organizations to keep their resources protected . in the current climate where more important information is placed online , authentication methods will help keep information protected.

REFERENCES

1. Burr, William; Dodson, Donna; Newton, Elaine (2011). "Electronic Authentication Guideline" (PDF). National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-63-1. Retrieved 3 November 2015.