International Journal of Emerging Engineering Research and Technology
Volume 4, Issue 3, March 2016, PP 27-33
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

SAMES-Secure Access to Multiple Entities via Smartphone

Ayush Saxena, Sourabh Pandey, Anurag Jain

Department of Computer Science, Sinhgad Institute of Technology, Lonavala, India

ABSTRACT

A new concept is proposed for a strong user authentication system. Users used to select short and simple passwords for their own convenience hence making their privacy susceptible to hacks. Possible attacks are shoulder surfing and key loggers. As a consequence, this architecture overcomes many limitations, thus making it a strong authentication scheme. In the purported scheme, password of the web entities such as Facebook, Gmail, twitter and so on is stored in the android smart phone. Whenever a user wants to log into the system, he need to login in the smart phone, in return the android application establishes the connection with the computer and the password gets verified using OTP (one-time password). The computer then opens the internet website and logs the user automatically.

Keywords: Smartphone, Credentials, Web Services, Password Security, Wi-Fi

INTRODUCTION

Most Internet services like e-banking, email and social networking implement control access with the help of password and username based authentication mechanism. Most internet services provide user’s different types of classes of passwords such as Visual, Graphical and Haptic. These have been offered to replace standard passwords. Textual passwords are the single way to authenticate a user to the Web. There is the possibility of getting knowledge of a user's password (e.g. By trial and error) and can compromise a user’s access to such services. The users are required to deliver a solid and secure authentication mechanism which will supply protection for the user’s credentials. Also for offering strong authentication we can apply the concept of the One Time Password (OTP). Password based authentication is more important for information protection. User authentication is frequently performed by asking a user for name and password combination. Some users create their own method for creating memorable multiple passwords through related passwords (linking their password via some common password elements) or sequence of queries. Thus, authenticating users in web and web based environments has been a problem for end users and network administrators. Hence, we are proceeding to examine how to resolve all these queries and manage secure transaction between Mobile and PC.

EXISTING METHODOLOGY FOR THE PAPER

Overview of SAMES

An overview of SAMES which includes the user accessing web services from the host machine via a smart phone. SAMES mainly concentrates on the interaction between host terminal and user when accessing the web service from the internet. A user chooses the strong password for the registering

**Address for correspondence:*

ayushsaxena1003@gmail.com

process of web service. It then stores credentials for the service, on smart device by manually entering this information. Whenever it has access to the web service, it securely transfers the credentials from a smart device to a host terminal or cloud storage which will then forward the credentials to the appropriate service providers [1].

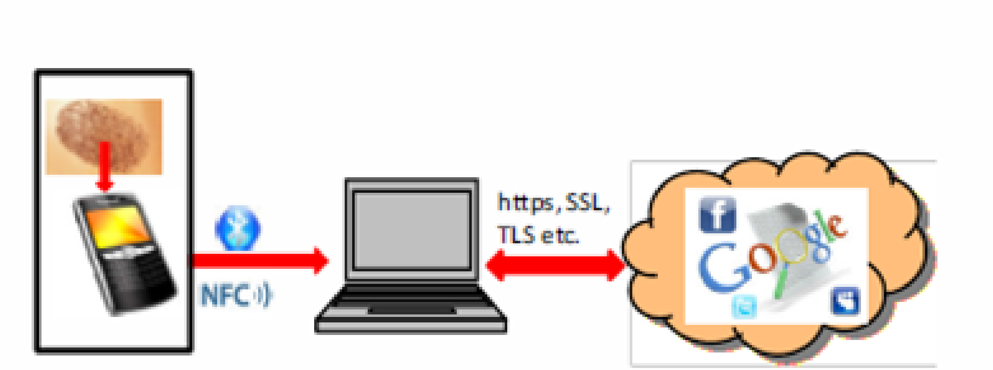


Fig1. *Overview of SAMES*

So as the result, the Service provider authenticates the user and delivers the service to the Host Terminal.

Aspects of SAMES

Building a secure system using insecure components and resilient against shoulder surfing and Key logger attack.

MITM Attacks for NFC

The use of NFC to transfer credentials attacks such as eavesdropping by using secure communication channels. The connectivity between device and host terminal eliminate the MITM attack.

DoS Attacks

NFC is not targeted by a DOS attack. Smart device could present a vulnerability to DoS attacks that aim at accelerating energy consumption [6].

Limitations of SAMES

Whenever the service provider is providing the service on the host terminal has possibility that the user may not available on machine in some emergency cases so to be sure that the presence of the user. We are trying to generate OTP between data transferred from Service provider to Host terminal. OTP is generated on the mobile phone when the service opening of the host terminal, through the OTP, we are sure that the actual user is available on the machine with including smart phone. Also, we can implement strong authentication with the most recent concept, is two-way authentication by using the One Time Password (OTP).

DESCRIPTION OF ARCHITECTURE

Integrating Biometrics using Smart Devices: In SAMES, the ubiquitous smart devices play a crucial role. Smart devices in addition to possessing the processing capability and memory that rival modern computers also have optimized modules to efficiently use their limited energy, thus providing longer standby time. Many smartphones. like the Samsung S7, comes equipped with biometric sensors like fingerprint readers as well as features such as face-unlock, to authenticate the use of the smartphone. This has resulted in a paradigm shift from the traditional password based authentication on computers to the use of biometric attributes for accessing personal data stored on smart devices. With the use of smart devices, the need for setting up dedicated Biometric authentication is not required, hence circumventing its major drawback. With such a secure system already in place, SAMES proposes to extend the existing authentication schemes present in the smart devices to access web based services [7][8]. By leveraging on smartphone authentication mechanisms, users can now authenticate themselves to web services via their smart device. Such a system provides an inimitable access to Internet services for each individual. By this we mean, only the owner has access to the credentials stored on the smartphone since the authentication of the device is tied to her unique biometric attributes and no other person can imitate these attributes. The “Grey Project” [9] also presented an access-control system based on smartphones that helps in authenticating a person while providing access control to physical resources such as a door.

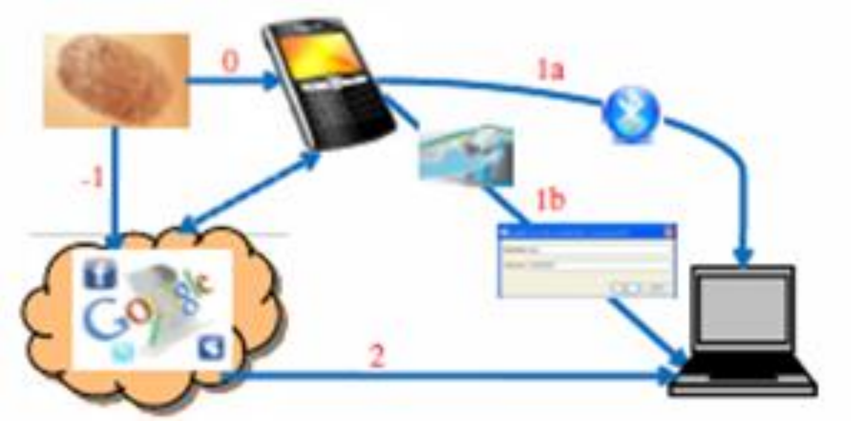


Fig2. *Operation of SAMES*

PROPOSED SYSTEM

In the proposed system, the password of the web application i.e. Facebook, Gmail and so on is stored in Android Smartphone. Whenever a user intends to log into the system, he clicks on the login button on the android application. In return the android application establishes a connection with the computer and on successful authentication transmits the password and the website. The computer then opens the website in the web browser and logs the user automatically into it [1].

Modules

1. Login & Registration (Android)

Using this module on the Android Smartphone, a new user can be created in the application. While creating a new user, the application captures necessary details related to the user. Whenever the user cares to log into the system next time, he will be authenticated using the credentials saved while registering the user for the foremost time.

2. Open Facebook uses Bluetooth/Wi-Fi (Android)

Whenever a user desires to access the Facebook, he clicks on the Facebook button and the system hits the browser and reverts with a text field asking the user to submit his password for Facebook.

3. Command Capture uses Bluetooth on PC (JAVA)

The desktop module securely captures command received using the android application. This request is processed and the subsequent module is launched for validating the user.

4. One-time Password Verification uses SMS (JAVA)

A one-time random password is generated by the Java application and it is transmitted to the user on his mobile telephone. The user needs to enter this password received on his android Smartphone to proceed with the process of login on the internet site.

5. Facebook Password Verification (JAVA+ Android)

Once the user is successfully validated by the one-time password, the application sends the login Credentials to the Java application for the login. The system automatically logs into the website with the credentials.

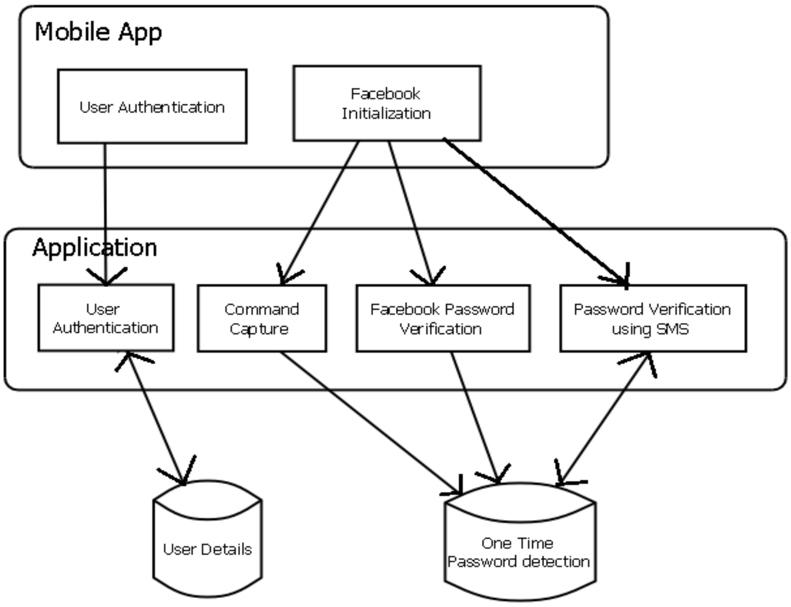


Fig3. *Architecture of SAMES*

The user will register into android application with username and password. These details will be stored into centralized application and also collect Personal identification data, which is really utilitarian. The user will login into android application using given username and password in Android Application. These will be authenticated using centralized application. After successful authentication, the user will be requested for Facebook credentials. These credentials will be stored in a centralized application. Now the user will select an option to open Facebook and select machine for Bluetooth connectivity, Java Application will request centralized application to generate one-time password. The centralized application generates one-time passwords and delivers it to the user via SMS. This password requested by android app to the user. The entered one-time password is transmitted to the Java Application by the android app for validation. The Facebook credentials are delivered to the android app and Facebook is opened on the browser using the specified credentials.

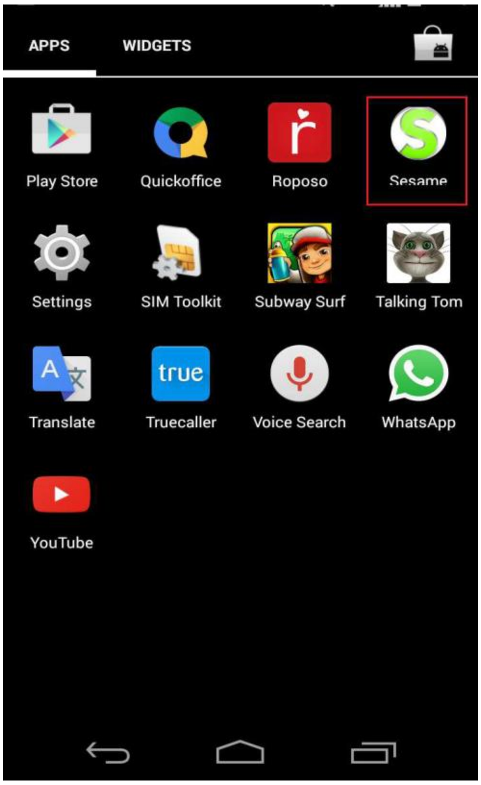
IMPLEMENTATION

1. SAMES Application installed on Mobile.
2. First user has to create a registration for accessing the Mobile application.
3. After registering this application user getting user id and password for accessing application next time.
4. The user will enter user id and password, click LOGIN.
5. On next time the user has to enter the IP address of the computer on which he/she want to open an account.
6. After entering OTP generation for confirmation that the user is actual or not.
7. Once the user gets OTP and enter then he/she will be on choosing service.

WORKING

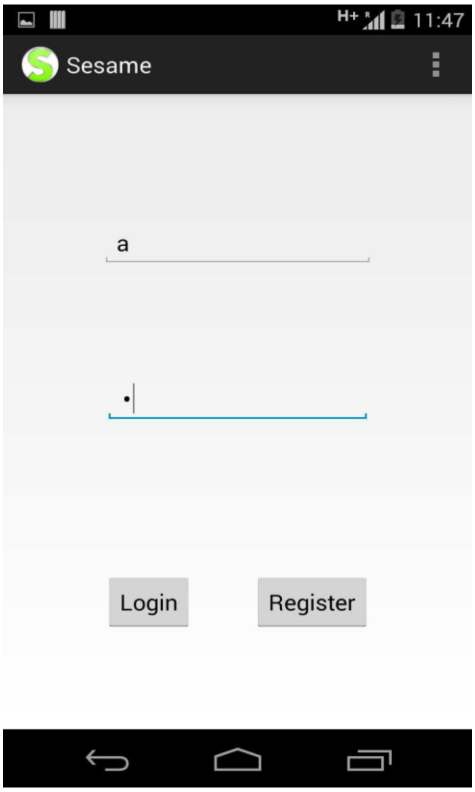
Step-1

Application Installed On Mobile



Step-2

After registration, user use user id and password for accessing this application.



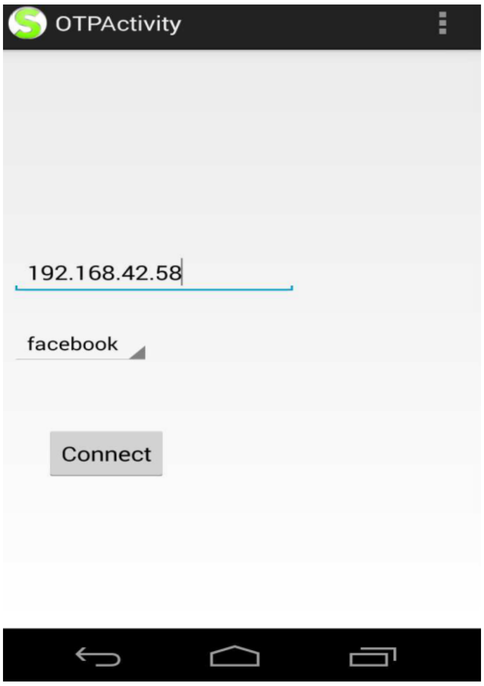
a

•

Step-3

User needs to enter the IP address of the computer on which he/she want to open an account.

As well he/she choose the service.

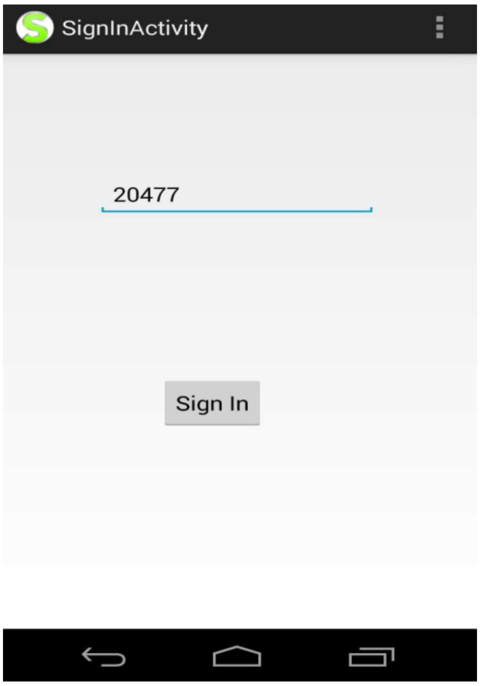


192.168.42.58

facebook

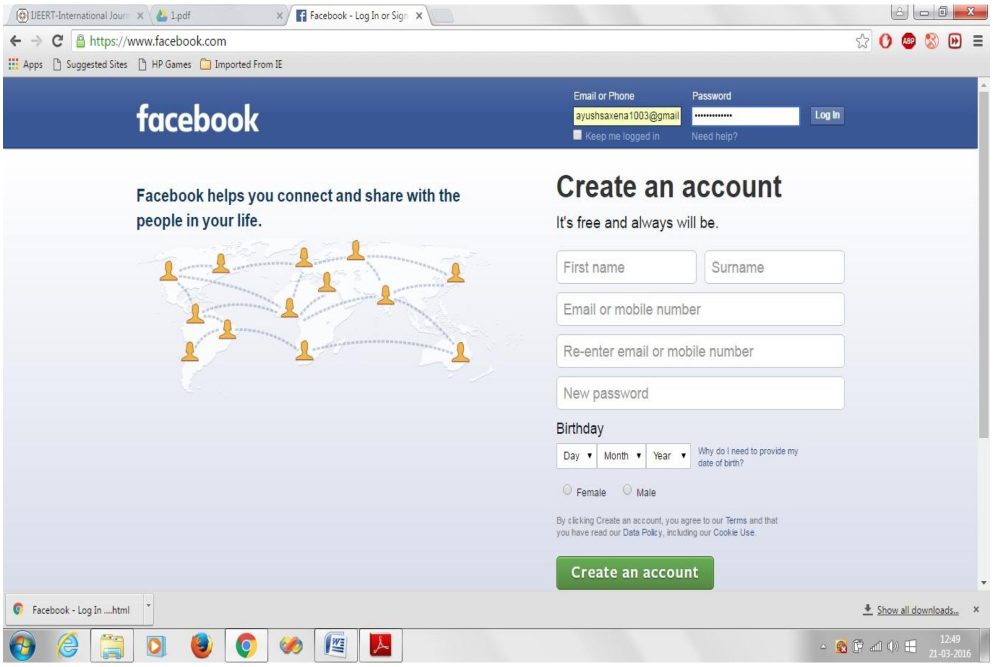
Step-4

Now it will jump on directly Facebook page and automatically type user id and password. The user does not need to type it manually.



20477

Hence, the user does not need to manually enter user id and password. It will automatically enter.



https://www.facebook.com

Email or Phone: ayushsaxena1003@gmail

Password: ••••••••••••

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

Why do I need to provide my date of birth?

By clicking Create an account, you agree to our Terms and that you have read our Data Policy, including our Cookie Use.

COMPARISON

Key	SESAME	SAMES
Name	Smartphone Enables Secure access to multiple entities via smartphone	Secure Access to multiple entities via smartphone
Technology	NFC	Wi-Fi
Authentication	One way No OTP	Two way with OTP
Algorithm	Simple Encryption	SHA-1 standard
Cost	More cost because of Biometric	Less cost because of ID and password system
Attack	Shoulder surfing, Key Logger attack are present	Shoulder surfing, Key logger attack are not present

ADVANTAGES

1. Incentivize the usage of strong passwords effortlessly.
2. Simulate emerging technologies such as smartphones into current technologies to realize a secure system.
3. This architecture eliminates all the shortcomings of textual passwords.
4. It aids in prevention of credentials from leaking out.
5. It prevents hacking from key loggers and shoulder surfing.

CONCLUSION

In the existing paper we have identified the problem of cost of project that for Biometric attributes. Also tried to give the service to user as when he/she physically present on host terminal. In addition to this including the concept related to OTP will provide two way authentications for the user. Service provider having guaranty that actual user is accessing the service. It is encouraging to the user set their password as a complex one. Also, there is no need to put same password for different services.

REFERENCES

[1] Amey Sanzgiri, Anandatirtha Nandudi, Shambhu Upadhyaya and Chunming Qiao " Smartphone Enable Secure Access to Multiple Entities" in 2013 International Conference on Computing, Networking and Communications, Internet Services and Applications Symposium.

[2] T. Van Do, et al, "Offering SIM Strong Authentication to Internet Services "White Paper, 3GSM World Cogress, Barcelona, February 2006.

[3] Maryline Laurent, Samia bouzefrane, Christophe Kiennert, "Towards a Secure Identity Management in Smartphone Environments"

[4] Do van Thanh, Tore Jonvik, Ivar Jorstad "Enhancing Internet Service Security using GSM SIM Authentication" full paper reviewed at the direction of the IEEE communications society subject Matter experts for publication in the IEEE GLOBECOM 2006 proceedings

[5] Audun Wangensteen, Lars Lunde, Ivar Jorstad "Secured enterprise access with strong SIM Authentication" proceeding of 10th IEEE International Enterprise Distributed Object Computing Conference 2006.

[6] S. Salerno, A. Sanzgiri, and S. Upadhyaya, “Exploration of attacks on current generation smartphones.” Procedia CS, pp. 546–553, 2011.

[7] A.Beaufour and P. Bonnet, “Personal servers as digital keys.” in Proceedings of the Second IEEE International Conf. on Pervasive Computing and Communications (PerCom’04), ser. PERCOM ’04. Washington, DC, USA: IEEE Computer Society, 2004.

[8] F. Zhu and M. W. Mutka, “The master key: A private authentication approach for pervasive computing environments.” in Fourth IEEE International Conf. on Pervasive Computing and Communications (PerCom06, 2006, pp. 212–221.

[9] L. Bauer, S. Garriss, and M. K. Reiter, “Efficient proving for practical distributed access-control systems.” in Computer Security—ESORICS 2007: 12th European Symposium on Research in Computer Security, ser. Lecture Notes in Computer Science, vol. 4734, Sep. 2007, pp. 19– 37.

AUTHOR’S BIOGRAPHY

Ayush Saxena, is pursuing Bachelors of Engineering degree from Sinhgad Institute of technology Lonavala. He is responsible for design analysis of system.

Sourabh Pandey, is pursuing Bachelors of Engineering degree from Sinhgad Institute of technology Lonavala. He is responsible for overall idea of system.

Anurag Jain, is pursuing Bachelors of Engineering degree from Sinhgad Institute of technology Lonavala. He is responsible for giving module idea.