INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 9, Issue 14, (2019) E-ISSN: 2222-6990

Discussion: Smartphone Authentication from Offline Remote Server

Moceheb Lazam Shuwandy, Mahmood Maher Salih, Ziadoon Tareq Abdulwahhab, Mohamed Aktham Ahmed

FSKIK,UPSI, MY, CCMS, TU, IQ, Malaysia

Email: p20161000220@siswa.upsi.edu.my, moceheb@yahoo.com

moceheb@tu.edu.iq

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v9-i14/6501 DOI:10.6007/IJARBSS/v9-i14/6501

Published Date: 25 October 2019

Abstract

Identity theft is one of the biggest challenges to protecting electronic devices, especially in protecting Smartphones. Authentication and its techniques are the most vulnerable to problems, such as traditional, pattern password and PIN code etc. In addition, biometric techniques are safer than normal authentication methods. Therefore, these techniques are related to the characteristics of human beings and used to authenticate who owns them. Besides, authentication is granted by a remote server to protect authentication data onto theft and manipulation. However, remote servers are vulnerable to problems such as hacker attacks, and systems and communications problems. On the other hand, the connection to the server should be available when requesting authentication from a Smartphone, otherwise the user will not be able to access his device. In this paper, we discuss the failure connected to remote server in order to obtain authentication, and some cases lead to non-authentication. We are discussing the user's access to the Smartphone by any biometric devices currently in use. When using of the local server if the remote server fails, by creating a Virtual Server (VS) on the Smartphone. For example: a user cans only access to his device, when obtain on the authorize form VS. It has the same specifications and environment, as the original server.

Keywords: Virtual Server, Authentication, Remote Server Failur, Smartphone.

Introduction

The biometric verification procedures, for example: face detection, retina scanning or fingerprint are viewed as more secure than the contemporary confirmation components, for example: smart card technology, even pattern locks, PIN or passwords in the cell phones. Regular verification instruments including graphical or alphanumeric passwords require that the client recalls the special blend of secret key. Additionally, the secrecy of the secret key is likewise a noteworthy worry in security frameworks. Secret key or PIN based verification instruments can likewise be broken by utilizing estimate or Brute Force dictionary. Biometric

validations give enhanced unwavering quality and ease of use in light of the fact that dissimilar to traditional techniques, it needs not to be recollected. Biometric procedures are either ordered as physiological (i.e. scanning of retina or fingerprint and so forth.) or behavioural, for example, voice. Additionally, Signature of Handwritten has a place with behavioural biometrics. It is one of the most established and most broadly utilized strategies for a person authentication on a document.

In other hand, the client–server demonstrate is an appropriated application structure that parcels assignments or workloads between the suppliers of an asset or administration, called server, and administration requesters called client. Frequently client and server convey over a cell phone arrange on independent equipment, however, both client and server may live in a similar framework. A server has run at least one server programs which share their assets with clients. A client does not share any of its assets but rather asks for a server's substance or administration work. Clients, hence, start correspondence sessions with servers which anticipate approaching solicitations. Cases of cell phone applications that utilize the client–server display are Email, arrange to print, and the World Wide Web.

This paper is aimed to build authentication far away from the user, in which the legitimate user is authenticated by sending the identify features to the Remote server. the smartphone connects to the server before using a secure authentication. The system of successful operation begins from Smartphone, the user access to his cell phone depends on one of security methods built in it. for example, some using one of the biometric technologies then it sends a request to the server. The server receives the data of authentication and makes process with a Data Base. the Data Base checks the data, Is available for this smartphone or not? After the server confirms that the authentication exists and matches what it has in the database, it returns the answer to the smartphone to allow the user to use the device. All this keeps the smartphone waiting for a server response, from request to response. See the figure 1. Below.

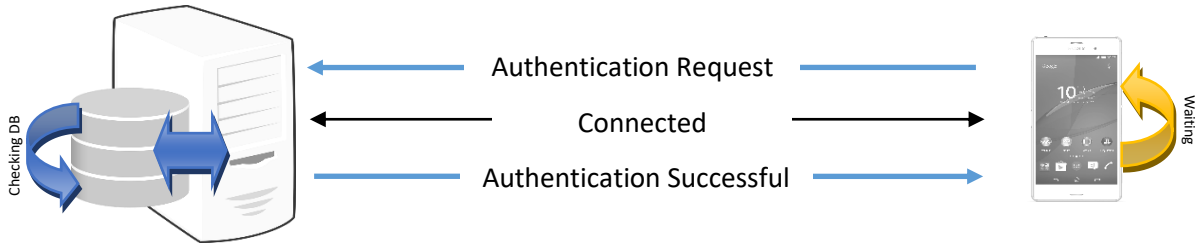

Figure 1. Show Smartphone connect by Remote server in successful Authentication.

Significant of Study

It is important to maintain the interest of the user for the purpose of continuing to use the product. In this paper, we seek to discuss the problem and the solution. The faulty connection to the remote server to obtain authentication or vice versa will prevent the authorized user from using his or her phone. For example, if someone uses the fingerprint, the smartphone will send the authentication request to the server. Which means that the person will be in a state of waiting until the response comes from the server. A person may be an elderly person, a patient, a child, a doctor, a banker, etc. In addition to keeping the connection to the server

at any time and the continuity of user access to the device and uphold the security of the smartphone.

Problem Background

The connection of the smartphone to remote server for the purpose of allowing the client to use it and determine whether it is authorized or not, is more security in terms of security. But the problem is in the first three directions in sending the request to the server and the second in the response of the server and the third in the carrier. The delay caused by any of the above three reasons does not guarantee the authorized person access to his system freely. Any security method, if feasible, is a failure.

Literature View

The verification information was blended with the protected information that was gathered all the while with the technique sort that utilized some time recently. It was watched that keep information in a memory of individuals in addition to the inconvenience that happens while overlooking the information is not a superior approach to genuine approve. Or, on the other hand, assault from who need to get to a gadget. Confirmation data made it safe in far away, utilizing a server to spare the data in the Data base. The trial was performed by volunteers who conveyed cell phone amid interface server. Another researcher was done to particularly recognize the direction of cell phone grabbing by utilizing one of the kind elements extricated from a Biometric innovation of cell phone.

Some researchers proposed framework engineering in view of three levels. To start with level is the client end. The client utilizes a cell phone to play out his mark noticeable all around. The cell phone is conveyed by the client in his grasp while he plays out the mark. The data of movement detected by the accelerometer is then sent to the server for confirmation. Server, which is the second level, applies coordinating calculation to distinguish the client.

Objective

The main objective of this paper is to build a temporary local server that matches the remote server in performance. The other thing is to keep the authentication outside of the smartphone, which would preserve the data without being able to access it without authentication. Besides, eliminate the loss of time that causes suffering to the user, especially in urgent and emergency situations.

Methodology

We discuss a way to solve the above problem, and how to find ways to eliminate the bugs. The system consists of a primary server and a temporary local server and a communication process between them.

The application to authenticate access to the smartphone connects to the remote server. The application will not allow the user to try to log in without a prior connection to the server, which makes it very troublesome if repeated failure to connect.

Local server(Virtual Server VS)

The local server has all the specifications of the original server, plus a small database containing only the authentication data of the smartphone. The application creates the first

local server after the first successful authentication with the remote server as shown in Figure 3, which explains the process of creating the local server. As follows:

1. The user uses the smartphone; the application connects to the remote server.
2. Successful connection.
3. Application The user is required to enter the technical means for the purpose of authentication.
4. The user enters, the smartphone says sending the authentication to the server for the purpose of matching.
5. The server receives the request and queries the database about the request.
6.When the process is completed, the server responds with a successful authentication.
7. Smartphone receives the answer of the server, and the application opens the device to the user.
8. The application creates the local server where it saves the successful authentication in the local database after encryption.
9. The connection with the server is closed after the end of the process of establishing the local server.

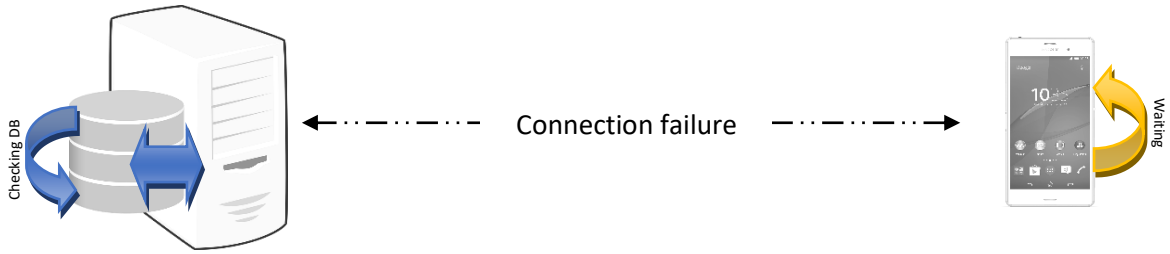

Figure 2. Show Smartphone in failure connection with the Remote server.

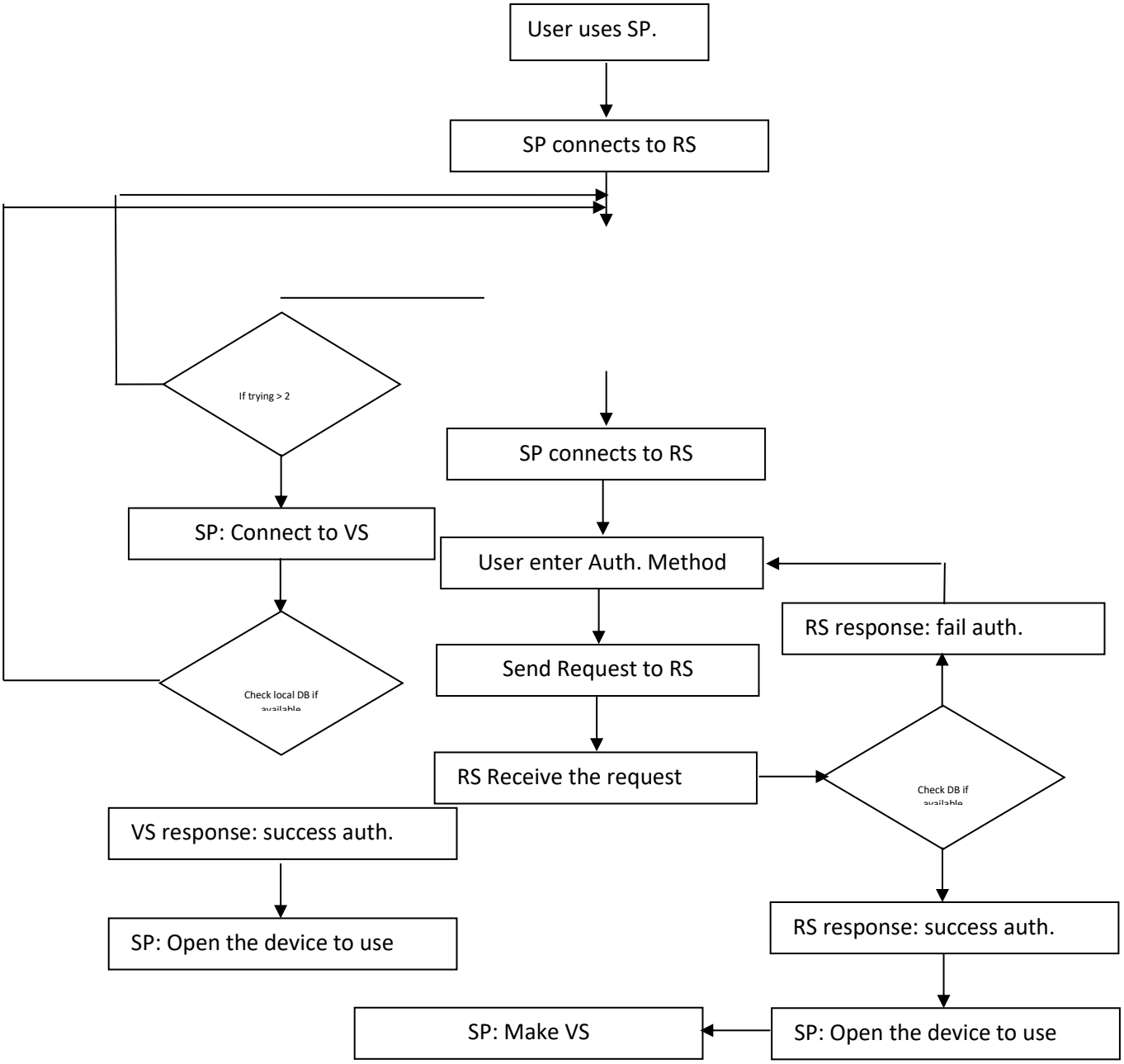

Figure 3. Flowchart show Smartphone (SP) connect to Remote Server (RS) and Virtual Server (VS).

When the remote server connection fails, the system makes the smartphone:
1. The user uses the smartphone; the application connects to the remote server.
2. Failed to connect to two attempts.
3. The application connects to the local server.
4. The connection was successful.
5. Application The user is required to enter the technical means for the purpose of authentication.
6. The user enters, the smartphone says sending the authentication to the server for the purpose of matching.

7. The server receives the request with the data after encryption and queries from the database about the request.
8. When the process is completed, the server responds with a successful authentication.
9. Smartphone receives the answer of the server, and the application opens the device to the user.

The application tries to connect to the remote server. When successful, they connect to the local server, check the data in the local database, and then say to change the internal data code after checking the data. In a case of incorrect login, the application says that the device is shut down until it is entered again correctly. See figure 3 above.

Discussion

Some researchers may say Why do not we skip the remote server at the local server? If we assume that we have done so, we will lose the local server in the first flaw in the smartphone system. This includes the result of a defect in the operating system or attack from hackers or because of some viruses and then it will cause great damage to the local server and disrupt the work in addition to absence access to information that was saved. In addition, the loss of the device means the loss of the local server, which means that the remote authentication is better in many cases can be a future study intended to develop a local server nearby not in the device itself, but in another device nearby and our study will cover it.

Conclusion

We discussed how to address the problem of lost connection between the smartphone and the server in devices that authenticate remote access. And the development of a mechanism for the purpose of reducing the dependence on the existence of connection to the remote server or not. However, this solution needs to be applied for the purpose of verifying the feasibility of its use. This depends on the environment and the mechanism used to determine the quality and specifications of all devices used.

References

Aviv, A. J., Sapp, B., Blaze, M., & Smith, J. M. (2012). Practicality of accelerometer side channels on smartphones. *Proceedings of the 28th Annual Computer Security Applications Conference on - ACSAC '12*. doi:10.1145/2420950.2420957.

Derawi, M. O., Nickel, C., Bours, P., & Busch, C. (2010). Unobtrusive user-authentication on mobile phones using biometric gait recognition. In *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on* (pp. 306-311). IEEE.

Doroz, R., & Porwik, P. (2011). Handwritten Signature Recognition with Adaptive Selection of Behavioral Features. *Communications in Computer and Information Science*, 128-136. doi:10.1007/978-3-642-27245-5_17.

Feng, T., Zhao, X., & Shi, W. (2013). Investigating mobile device picking-up motion as a novel biometric modality. In *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on* (pp. 1-6). IEEE.

Guerra-Casanova, J., Avila, C. S., Bailador, G., & De-Santos-Sierra, A. (2011). Time series distances measures to analyze in-air signatures to authenticate users on mobile phones. In *Security Technology (ICCST), 2011 IEEE International Carnahan Conference on* (pp. 1-7). IEEE.

Laghari, A., & Memon, Z. A. (2016). Biometric authentication technique using smartphone sensor. In *Applied Sciences and Technology (IBCAST), 2016 13th International Bhurban Conference on* (pp. 381-384). IEEE.

Shuwandy, M. L. (2013). Smile Mask to Capsulation MOLAZ Method. *International Journal of Computer Science and Network Security (IJCSNS)*, *13*(12), 66.

Vildjiounaite, E., Makela, S. M., Lindholm, M., Riihimaki, R., Kyllonen, V., Mantyjarvi, J., & Ailisto, H. (2006). Unobtrusive multimodal biometrics for ensuring privacy and information security with personal devices. In *International Conference on Pervasive Computing* (pp. 187-201). Springer, Berlin, Heidelberg.

Weiss, G. M., & Lockhart, J. W. (2011). Identifying user traits by mining smart phone accelerometer data. In *Proceedings of the Fifth International Workshop on Knowledge Discovery from Sensor Data* (pp. 61-69). ACM.

Yeh, K., Lo, N. W., & Li, Y. (2010). Cryptanalysis of Hsiang-Shih's authentication scheme for multi-server architecture. *International Journal of Communication Systems*, *24*(7), 829-836. doi:10.1002/dac.1184