American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-7, Issue-6, pp-140-142
www.ajer.org
Research Paper Open Access

System Model andMultifactor Authentication forSecurityofmobile BankinginSri Lanka

Wijenanda D. A. K.[1] Sellappan Palaniappan [2]
Malaysian University of Science and Technology, Malaysia[1,2]
***Corresponding Author: Wijenanda D. A. K*

ABSTRACT:*The conceptual architecture of a proposedmobile app model was presented in a paper published in a journal by Wijenanda and Sellappan (2018). The basic conceptual architecture was presented in that paper. This paper covers the successfully developed architecture for the mobile application. In particular, the systems model and the multifactor authentication architecture are presented in this paper. The presented set are based on the developed application. The system's model describes the flow of data, which includes the input of data, fetching of the data from the database, validation of inputted data and validated result. The components of the model include authentication, configuration management, PIN comparator, Face Image Processor, Voice Processor, Face Image Comparator, Voice Comparator and Parameters component. For the multifactor authentication architecture, security Level Selector accepts PIN, Voice and Face as inputs for authentication check. The face and voice processor take the face and voice inputs and process and pass to the next stage. The next stage is that of validation, where the PIN, voice and face are validated before successful authentication. The mobile application is being developed as a prototype based on this architecture.*
KEY WORDS:*Mobile application, Mobile Banking, System Model, Multifactor Authentication, mobile phones.*

Date of Submission: 28-05-2018 Date of acceptance: 11-06-2018

I INTRODUCTION

Breath-taking pace of evolution in communications technology and the correspondingchange in consumer behaviour has had a significant impact on how customers perceive anduse banking services (Sunari, 2014). The growth of mobile technology and the ever-growing ubiquity of mobile devices over the years, have resulted in mobile banking to come up from a simpleinformation delivery channel to that of a comprehensive banking transaction channel. In mobile banking schemes; financial services are availed and banking services are provided using mobile devices (Baraka et al, 2013).The challenge now for Sri Lankan banks is to develop and execute a mobile banking strategy that creates value for customers and encourages them to switch to the mobile channel from the costlier channels such as branch, so that it would make a difference to the cost/income ratio of the banks (Sunari, 2014).

II LITERATURE REVIEW

In pursuit of objectives like secured banking, financial institutions globally have placed heavy emphasis on cost effectiveness, efficiency and seamless service and the optimal mobilization of existing resources and infrastructure (Delrene, 2016).Experiences of several developing countries have shown that the poor majority are in need of a wide range of financial services that could potentially be delivered via mobile phones or mobile phone operators. In their operations, these mobile apps send data in plaintext. Financial service providers tend to rely on the security services provided by the mobile applications, which has been proved to be susceptible to cyber-attacks. The used algorithms for crypto mechanisms are flawed leaving data carried through the network vulnerable upon interception.

Banking operators need to take precaution by enforcing some protective measures on the information to be transmitted. This is beside the security required to be incorporated into the mobile apps in terms of the authentication of the platforms. Access to banking services widely acknowledged to be high and financial access in Sri Lanka being estimated between 68.5% of population (WB) to 82.5% of households (GTZ), 58% of adults of bottom 40% income group having bank accounts (WB) is a call for security improvement (Peter, 2013).The

banks in Sri Lanka, however, are trying to popularize the concept of Internet banking among their customers, to meet up with the ever-increasing traffic in physical bank premises (Kariyawasam, 2016).Mobile phones have created a platform to expand commercial transactions in a very easy manner and have created a wide array of business opportunities through the expansion of wireless communication (Kumari and Janaka, 2014).The basic idea of mobile services is to improve the access of information services when travelling or anywhere (Drennan and Mort, 2007).

In a case where a banking area is poor in terms of internet connectivity, there will be need for proposing a topology for improving the connectivity. These could begin with a preplan for a better topology (Datukun et al, 2016a; Datukun et al, 2016b). Improving network performance is necessary in any organization (Datukun et al, 2017). This include tourist centres for freely and conveniently connecting virtual tourism. With the increasing levels of deployment of various forms of high-speed (or broadband) services within today's Internet, there is new impetus to find some usable answers that allow both providers and users to place some objective benchmarks against the service offerings. Furthermore, with the lift in access speed with broadband services, there is an associated expectation on the part of the end user or service customer about the performance of the Internet service. It should be "better" in some fashion, where "better" relates to the performance of the network and the service profile that is offered to network applications. And not only is there an expectation of "better" performance, it should be measurable (Onwudebelu et al, 2014).This will help in browser-based management information system provided for administrative users in mobile banking.

III METHODOLOGY

This research is a project aiming at improving the security situation of mobile banking in Srilanka. Apaper has been published by Wijenanda and Sellappan (2018)with an initial architecture based on literature review on the idea. That was towards developing a mobile application with biometric security for authentication. This paper, in connection with the last paper presents the system's model and MultifactorAuthentication architecture based on the reviewed concept. Based on the methodology diagram from Wijenanda and Sellappan (2018), the actual system's architecture and Multifactor Authentication architecture follows.

Mobile System's Model and Multifactor Authentication architecture

The applicationresident in customer's mobile phone is being launched before logging into the application server.The transaction is then initiatedbefore biometric recognition. It is after the biometric recognition that the customer will be allowed to access the account for relevant transaction (Wijenanda and Sellappan, 2018). The biometric recognition shall be by the customers' face, voice and customer's PIN. Since no two people's face are exactly the same and would further improve the security platform of the mobile banking in terms of hacking and other security threats and / or risks in terms of the difficulty to break the three authentication requirements. Figure 1 describes the System's modelwhich includes the input of data, fetching of the data from the database, validation of inputted data and validated result. The components of the model include authentication, configuration management, PIN comparator, Face Image Processor, Voice Processor, Face Image Comparator, Voice Comparator and Parameters component. For the multifactor authentication architecture, security Level Selector accepts PIN, Voice and Face as inputs for authentication check. The face and voice processor take the face and voice inputs and process and pass to the next stage. The next stage is that of validation, where the PIN, voice and face are validated before successful authentication. The mobile application is being developed as a prototype based on this architecture.

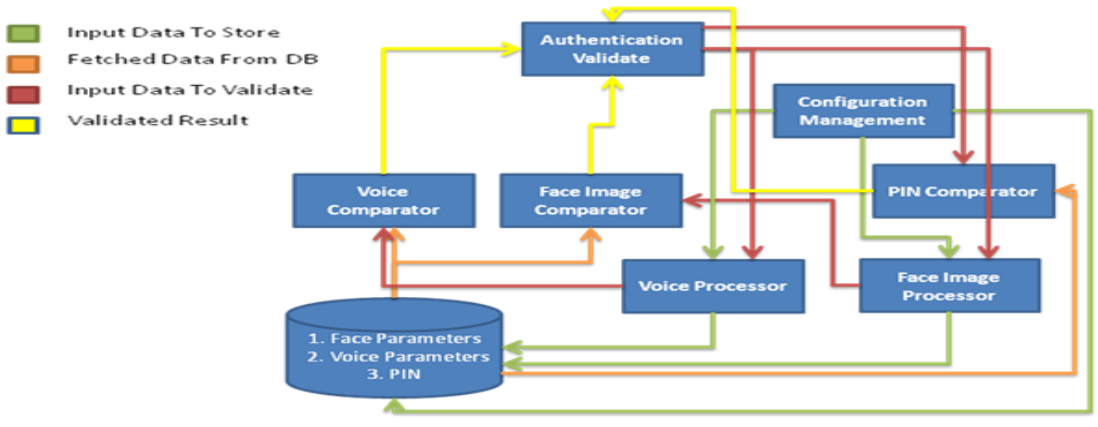

Figure 2: System's model

Figure 2 describes the multifactor authentication architecture, which clarifies on the authentication procedure. The authentication requirements are also indicated.

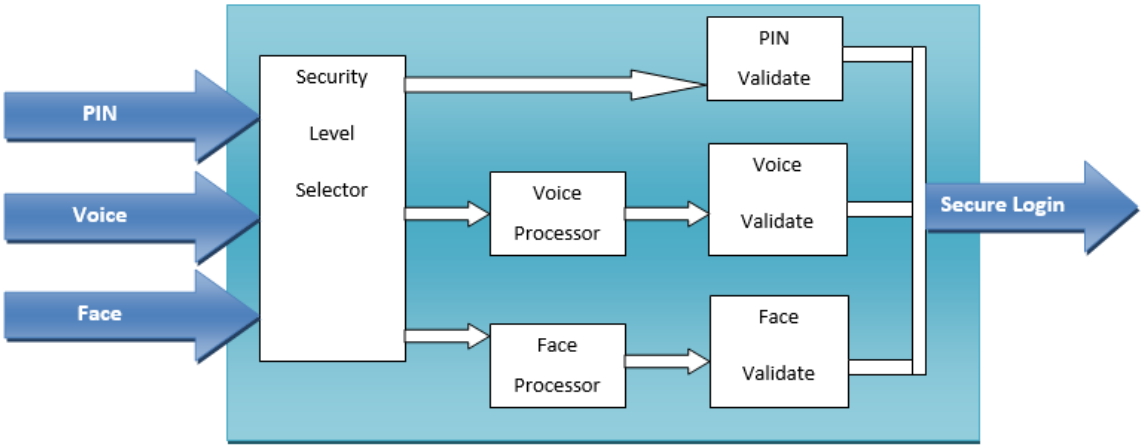

Figure 1: Multifactor Authentication

IV CONCLUSION

In as much as the system's model and the multifactor authentication architecture are important, the actual protype is also important. The protype has been developed based on the given system's model and multifactor architecture but require finetunement and Quality check testing. In the subsequent part of these work, which is the next work, shots of running application will be presented. This will be towards a user study to check whether the given solution is viable to improve mobile banking, particularly in the bank under study. Hence, we could conclude that this modelwill subsequently provide a mobile application with improved security. As such the next paper will be in connection to this one.

REFERENCES

[1]. Sunari Dandeniya (2014). Expanding Financial Services Frontier and Mobile Banking in Sri Lanka. 26th Anniversary Convention.
[2]. Baraka W. Nyamtiga, Anael Sam and Loserian S. Laizer (2013). Enhanced Security Model for Mobile Banking Systems in Tanzania. International Journal of Technology Enhancements and Emerging Engineering Research. 1 (44).
[3]. Delrene Seneviratne (2016). Mobile Banking as a Channel of Financial Inclusion an Urban Case Study. 28th Anniversary Convention
[4]. Peter Lovelock (2013). Mobile Payment in Sri Lanka: Market Demand Assessment. TRPC.
[5]. N. J. Kariyawasam and Nuradhi K. Jayasiri (2016). Awareness and Usage of Internet Banking Facilities in Sri Lanka. International Journal of Scientific Research and Innovative Technology. 3 (6).
[6]. Kumari Kahandawa and Janaka Wijayanayake (2014). Impact of Mobile Banking Services on Customer Satisfaction:A Study on Sri Lankan State Commercial Bank. International Journal of Computer and Information Technology. 3 (3).
[7]. G. Drennan and J. Mort, J. (2007). Mobile Communications: A Study of Factors Influencing Consumer use of m-services. Journal of Advertising Research. 47 (3). 302-312.
[8]. Datukun KalambaAristarkus, Sellappan Palaniappan, TatchanaamoortiPurnshatman (2016a). Towards proposing network topology upgrade in Salem University Lokoja. Research Publish Journals 4 (3).
[9]. Datukun KalambaAristarkus, Sellappan Palaniappan and TatchanaamoortiPurnshatman (2017). Hybrid Topology Design for Improving Network Performance. Global Journal of Computer Science and Technology: ENetwork, Web & Security. 17 (3).
[10]. Datukun KalambaAristarkus, Sellappan Palaniappan, TatchanaamoortiPurnshatman (2016b). Graph Model for Physical Topology Design. IASET: Journal of Computer Science and Engineering (IASET: JCSE)ISSN(P): Applied; ISSN(E): Applied. 1 (2).
[11]. Onwudebelu Ugochukwu, Datukun KalambaAristarkus, S. E. Adewumi (2014). Diagnosing Salem University Lokoja Network for Better Network Performance. Universal Journal of Communications and Network. 2(2). 40 – 46
[12]. Wijenanda D. A. K. and Sellappan Palaniappan (2018). Towards Improving Security for Mobile Banking in Sri Lanka. International Journal of Financial Management (IJFM). International Academy of Science and Engineering Technology (IASET). 7(3). 9-14.

Wijenanda D. A. K."System Model and Multifactor Authentication for Security Ofmobile Banking in Sri Lanka."American Journal Of Engineering Research (AJER), Vol. 7, No. 6, 2018, PP.140-142.