Journal of Computer Science

Original Research Paper

Multi-Factor Authentication for e-Government Services using a Smartphone Application and Biometric Identity Verification

Mohammad AlRousan and Benedetto Intrigila

Dipartimento di Ingegneria dell'Impresa, University of Rome "Tor Vergata", Italy

Article history
Received: 04-12-2019
Revised: 07-02-2020
Accepted: 19-02-2020

Corresponding Author:
Mohammad AlRousan
Dipartimento di Ingegneria
dell'Impresa, University of
Rome "Tor Vergata", Italy
Email: Moh.rousan1983@gmail.com

Abstract: The growing usage of smartphones and tablets has a significant impact on e-government services, according to Cisco and accounted for 59 percent of total IP traffic during 2018. In the provision of e-government services, usernames and passwords are still the most common authentication scheme. A password, however, is a weak authentication scheme, as it can easily be hacked over an insecure network connection. Therefore, a robust security solution for data in transit is becoming increasingly necessary. This paper proposes an authentication scheme that integrates multi-factor authentication procedures, a One-Time Password (OTP) and biometric authentication ("facial recognition" or "fingerprint") for the unified authentication of users before allowing them to access e-government services via a self-enrollment process.

Keywords: Mobile Applications, One-Time Password, Multi-Factor Authentication, E-Government Services, Biometric Identification

Introduction

Currently, the use of e-government services is increasing for public administration across the globe. Della Penna *et al*., 2019) pointed out that e-government is not about developing a static website with information for citizens; instead, it is a new era of citizen and government relationships and engagement. For public administration, e-government represents an opportunity to improve the quality of public services and reduce deficits, while from another perspective, citizens expect high-quality, secure and transparent e-government solutions. Although the new digital way of doing things offers advantages such as faster, more convenient services and efficiency in providing these services, the systems also present security challenges to government and users (Centeno *et al*., 2005). According to Cisco (2019), smartphones accounted for 59 percent of total IP traffic in 2018, accounting for approximately 2.4 zettabytes.

Smartphones are becoming a must-have gadget in daily life. Sending SMS verification codes to users presents a convenient option to send instantly generated passwords to users. However, the fact that the government does not control mobile phone services introduces a challenge the government agencies providing these services since they remain at the mercy of mobile phone service providers (Della Penna *et al*., 2019). If these companies fail to deliver the required level of service, it is the users of government services who suffer.

Hence, safety and user authentication are factors influencing the usability of smartphones for accessing e-governments services. In current e-government systems, users are requested to apply a two-step verification mechanism. This involves the use of a username and password as the first step and an automatically generated One-Time Password (OTP) to authenticate users' access to a government services as the second step; the OTP layer has been established as an extra layer of security (Dmitrienko *et al*., 2014). However, this two-step verification mechanism still lacks assurance regarding users' identity verifications, which represents a significant challenge affecting most information systems across the globe; insecure networks are often compromised and attackers steal data.

In this paper, a new model is proposed that integrates multi-factor authentication procedures, an OTP and biometric authentication ("fingerprinting" or facial recognition) for unified authentication of users before allowing them to access e-government services.

The paper starts with a brief discussion of the key challenges facing government entities and the main components of the new proposed model, i.e., OTPs and biometric authentication and continues by identifying the benefits of biometric verification. This is followed by a discussion of the current security challenges of using traditional authentication procedures using standard passwords and usernames. The paper concludes with a detailed description of the proposed authentication solution.

Science Publications

Literature Review

Authentication and IT Security

IT security is an area of research that has received significant interest in the last two decades or so. The main reason for this is the massive growth of the IT sector and the huge role it is increasingly playing in society. Currently, the vast majority of government institutions and private corporations are automating their services and IT systems are at the heart of these exercises (Hashizume *et al*., 2013, p. 5). This trend will not change soon, given the competitive advantage IT systems offer these organizations. Besides, these IT systems guarantee things such as faster services, efficiency of services and improved services from several organizations where bureaucracy and delays have been the order of the day for centuries. While IT has delivered these advantages and promises even greater things, it faces enormous challenges that cannot be ignored by IT system developers. Hacking and cyber-attacks have been on the increase (Thirumalai and Budugutta, 2018). Cyber-attacks have necessitated the need to improve IT security in all information systems, especially in government institutions where personal and sensitive information is often used and stored. Failure to guarantee IT security is synonymous with the collapse of the entire system.

In today’s world, the legacy authentication process based on static passwords is considered a vulnerable authentication mechanism (Stanislav, 2015). A combined mechanism presented by combining the static factor (password only) and a multi-authentication factor that depends on an OTP (IETF, 1998) or a biometrics authentication factor (Velásquez *et al*., 2018) is more robust and trusted.

Due to the urgency and sensitivity of the subject in question, developers of IT infrastructure have taken steps to counter the issue of attacks and the possibility of hacking by improving security issues across information systems installed for use by the public. Measuring the security of a system is achieved in terms of its ability to allow only entitled account holders access to a system while denying illegitimate access to people with malicious intent. Systems can achieve this level of security by having clear procedures for identifying people trying to access the system and clear authentication procedures that are safe and not prone to compromise. The system proposed by this paper, whereby an application will be built to enable secure authentication by increasing security around the authentication processes, seeks to address this very issue.

IT security is also critical given the cost of having insecure systems. Billions of dollars have been lost to hacking and cyber-attacks by both large and smaller organizations around the globe (Cashell *et al*., 2004). The cost of addressing successful attacks may be too high even for government organizations to address. Therefore, it is prudent for e-government services to be secure and steps should be taken to ensure that the implemented systems are carefully vetted for safety before users can use them. The systems also have to be simple enough for use by people with average knowledge of IT systems. While simple systems with advanced security mechanisms represent a combination that is extremely hard to achieve, it nevertheless has to be done, given the risks involved and the potential cost not achieving this.

One-Time Password (OTP) Authentication

Authentication is the assurance that the communicating entity is the one it claims to be. An OTP is one of the most used authentication procedures today. It is randomly generated by secure servers for use by the end user within a specific time slot. If the code is not used in the specified time slot, then it will expire and become invalid for the user’s authentication, which makes the OTP a secure mechanism for verification purposes. Attackers who may want to replicate OTPs will find them useless after a short while (Yeh *et al*., 2002).

Contrary to traditional forms of authentication that only required a user to access a system using a username and a password, this system can be beneficial if used correctly (IETF, 2005). An OTP can be generated by two methods. The first method involves the use an OTP algorithm, using hash functions and pseudorandom number generators to ensure high-level encryption and also ensure that the guessing of password predictions is extremely difficult, if not impossible (Thirumalai and Budugutta, 2018).

The second method involves using time-synchronized systems algorithms, which represents the most popular methods for generating OTPs. In this method, the OTP is created by making use of current timestamps and using the previous password or secret keys (Nag *et al*., 2014).

The most common algorithm, the Time-based OTP (TOTP), makes use of both the current timestamp and a shared secret (often user information such as an ID number or address). A cryptographic hash function is then used to determine the OTP (Huang *et al*., 2011; Law and Yam, 2007; IETF, 2005; 2011; Thirumalai and Budugutta, 2018).

The use of OTPs is essential in the implementation of multi-factor authentication systems. In e-government services, it has been used over the last two decades. However, the most popular means of getting this generated OTP to the user is through use of SMSs (Mulliner *et al*., 2013). Since most people have access to mobile phones, the use of these phones as a way to access the generated password makes sense.

However, this system is not without its disadvantages. The most common disadvantage is that the speed of message delivery is dependent on the efficiency of the user's mobile phone network. If the network is inefficient and causes delays in delivery for some reason (Ashfield, 2016; Weir *et al*., 2009), then the user is likely to find it hard to access the system because of the expiry feature of these passwords.

The second challenge is that the government institution does not have control of the data and data security is dependent on the network servers through which these SMSs are delivered (Ashfield, 2016; Della Penna *et al*., 2019; Weir *et al*., 2009). Moreover, cyber-attackers can intercept the transmission of SMSs if they target smartphones (Leavitt, 2011). The third challenge is associated cost of OTP SMS transactions from the server to users, which are usually paid to mobile operators by the end user.

Biometric Identity Verification

With the growing need for robust authentication schemes, the use of biometric-identity-verification-based systems has become widespread (Wang *et al*., 2003). Biometric identity verification systems propose a new key that is user-friendly, intelligent and reliable for user recognition systems by capturing users' fingerprints or facial patterns (Bremananth and Chitra, 2006). Apart from OTP generation, which ideally guarantees the user secure log-in sessions, a biometric identity verification feature also ensures users' security in accessing their data (Ashbourn, 2014). Fingerprints and facial biometrics are unique to every person because the pattern is encoded at the interface between the dermis and epidermis. Even a person's left and right five fingers have completely different print patterns (Browne, 2010). Hence, biometrics are unique, secure and living passwords to verify the integrity of transactions.

In today's world, most government entities tend to improve the identification process by linking each identity document or travel document with a unique biometric, following the International Civil Aviation Organization's (ICAO) standards. Only the digital image of a person is stored in both identity cards and passports as a JPEG or JPEG2000 as part of the ICAO standards and can be considered as public data that does not require a private key to be read. Further, most new smartphones are equipped with facial and fingerprint recognition methods to allow users to access their smartphones. Those additional features can support governments in simplifying identification and authentication processes to allow users to access government services (European Commission, 2018; ICAO, 2015).

Conceptual Model

Overview

This paper presents a new conceptual model to develop an OTP mobile application that can be installed from a trusted government-secured zone through kiosks distributed over governmental Post Offices to ensure full control by the government. It is meant to ensure that the app installation process is secured and controlled by the high security standards imposed by governments.

The app can be installed without any human interaction or involvement from any government personnel. The process will offer the app to users and verify their identities before installing the application on their smartphones. Automated identity verification via biometrics introduced at kiosks will be provided by facial and fingerprint recognition devices along with identity-card readers. Figure 1 illustrates the conceptual model for multi-biometric verification using a mobile app installed through kiosks.

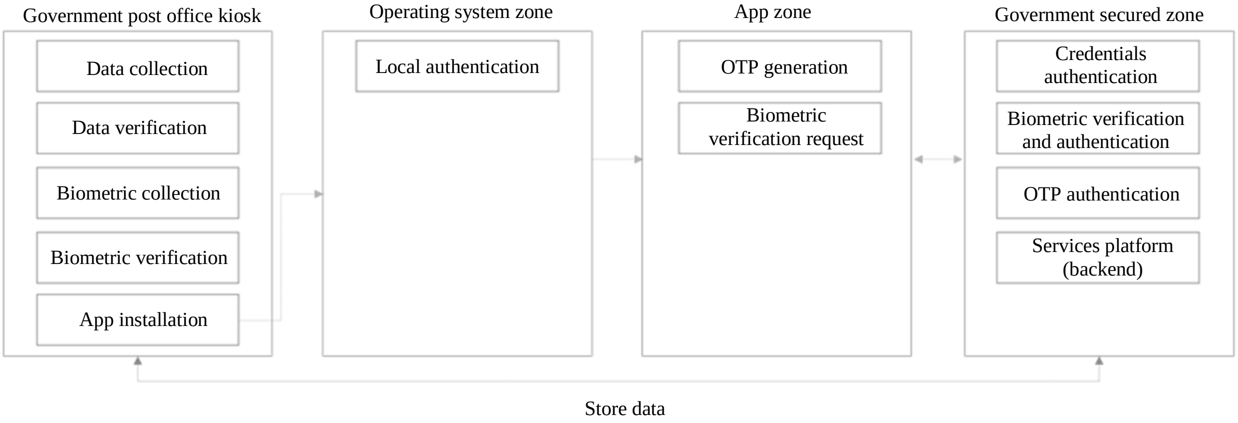

Fig. 1: Conceptual model

OTPs generated in the app do not provide attackers opportunities to easily intercept them, since the app being built will solve the problem of generation and transmission, as the users' smartphones will generate the OTPs instead of using a backend server for OTP generation. The OTP result will be shared with the government-secured zone along with user information to validate the transaction performed in addition to the user identity biometric for an extra layer of security checking. The user transaction that will be completed will be secured using the OTP on the app-zone side and the biometric checks on the government-secured-zone side to ensure a high level of security and audit being performed before completing the transactions.

Additionally, only basic knowledge of the use of smartphones will be required. The app's generation of OTPs will be done internally using secret keys that will be a combination of the current timestamps and the user's information that the application will have regarding the user and the mobile's IMEI. The conceptual model consists of the following zones:

- **Governmental Post Office kiosk**: Will represent the only real engagement point between the user and the government to collect a user's data, biometrics and personal mobile IMEI where the app will be installed. It will also serve to verify the user's identity in a fully automated way using a pre-installed identity card or passport reader and through facial- or fingerprint-recognition devices. Once positive results are retrieved, the app can be installed directly from the kiosk to ensure a high level of security
- **Operating system zone**: As an initial security step, users must access their mobile phones using their biometric authentication feature
- **App zone:** The app generates an OTP that links with the user's biometrics, personal information and IMEI using TOTP algorithms to generate a secret key that will be shared with the government-secured zone. Also, the user's live facial image or fingerprint is collected at this time. Every time the user accesses the app, the collected biometric will be shared with the government-secured zone
- **Government-secured zone:** Here, the credentials authentication, OTP authentication and biometric verification and authentication will be performed. The results of the authentication mechanism at the government-secured zone will allow the user to complete the services on the government services platform in addition to the online platform where users can submit service requests to the government through any available channels that the government has, either mobile applications or online government portals

Process Details

The process of acquiring the app is just as important as the app itself. The installation procedure is fundamental to the security issues that the model addresses.

Step 1 (User Registration)

The first step will involve user registration without the need to physically visit government offices, which can be done through the e-government services portal. At this stage, users will enter their details, such as name, identification number, postal code and other information such as gender, nationality and date of birth. The first step will allow users to have an account with the system that will be subject to verification. At this stage, users can obtain a username and password and their email address can be registered with the e-government services platform along with their necessary identity information.

Step 2 (Identity Verification and Enrollment)

The second step will involve users having to physically visit a governmental Post Office install the app. In this step, the details entered online will be confirmed and verified by the automated identity-verification process. Users should insert their identity document, whether an ID card or passport, into a document-reader device installed at a kiosk. Then the system will compare the details previously provided via the online platform (Step 1) with the identity details from the provided document. Then, users will be requested to stand in front of a facial camera for automated identity verification using the stored facial image from their identity card or passport. Further, users will be requested to place two fingers in the fingerprint scanner installed at the kiosk. Finally, the facial image and fingerprints will be registered in a fully encrypted database and matching engine to allow users to access government services in the future once their identify is confirmed.

The main reason for users to visit the kiosks to perform these necessary procedures is to use trusted networks to ensure the overall security objective. The government network is a trusted network where downloads and verification procedures can be secured, minimizing chances of attacks minimized. Conversely, free downloads over insecure networks can be intercepted and useful information obtained by attackers. Also, the purpose of the visit is to enroll their biometrics; however, users can opt out of the biometrics enrollment if they wish.

Step 3 (App Installation and Activation)

The app installation will not be available through public application markets such as Google Play. Instead, the application will only be made available to users from the government-controlled kiosks, which can be installed in governmental Post Offices or similar network locations secured and trusted by the government. Users will be asked to plug their smartphones into the kiosks for installation, which can be done only for users who have already registered online and have completing the identity verification at the same kiosks.

The app-installation phase and identity verification will also capture other essential details useful for this entire exercise. The user's smartphone details, such as the phone's IMEI number and brand, can be obtained and recorded during the app-installation process. Obtaining these features enables the smartphone to be uniquely configured and identified when the user tries to log into the government services platform later on to access government services. Also, the IMEI number, together with other personal details from the user acting as the security keys, can be used in the random generation of the OTPs.

App management will also be part of the security measures that will guarantee security for the application. Since the application will not be available from public stores, potential hackers cannot gain access to the app's installation codes to manipulate them to their advantage. Applications stored in public stores and freely available for download always pose this risk, whereby malicious people can clone the application and use the cloned apps to steal user data.

Before the user leaves the government administrative offices, the entire process will be verified by the user logging into the system, generating use of the app and safely logging into the system. If this is achieved, then it is assumed that the entire app-installation and identity-verification processes were successful and the user can now securely access the e-government services from the comfort of home. Figure 2 presents the application installation process.

These details highlight the imperative nature of the exercise and the need to carry out the activity at the government offices through dedicated kiosks where access to the trusted network is limited and access is secure. This will minimize the chances of later attacks and the possibility of attackers cloning the user's application without having access to the user's hardware (smartphone) and other security features only known to them.

Application Use

The application will have the OTP and biometric identification features as security measures. Both features will form the multi-authentication layer on top of the static password factor.

As a first step, users can obtain a random OTP generated from information gathered during the installation process, timestamp and user-registered mobile phone, such as the IMEI. An algorithm will be used to generate an OTP on the mobile app along with a secret key, which will not be shown to the app user. The secret key will be synched with the government-secured zone.

For the second step, once the OTP is generated, the app will require that users undergo biometric identification using their mobiles and the collected biometric images will be encrypted and shared with the government-secured zone for identification purposes. If a positive match with the registered identity during the installation process and an OTP authentication are positively confirmed, then the government-services platform will allow users to complete the service they intend to perform on the platform without having to enter any OTP code on the platform.

The biometric identification system is one of the most secure identification procedures, with applications in a wide variety of fields. Since biometrics are unique to every person, facial- or fingerprint-dentification procedures will prove to be a shrewd security feature that ensures the proposed model is highly secure and less prone to common forms of attack. The identity-verification process will be performed at the government-secured-zone level, using matching algorithms in the backend system. Figure 3 represents a sequence diagram of the application installation.

The speed of improvement in technology inspired the inclusion of biometric identification features in the proposed conceptual model. Only a few years ago, the average smartphone did not have facial- or fingerprint-identification features. Now, the facial-identification feature has been included in most smartphones and it is expected that it will soon be essential for all smartphones to have this feature. The biometric-identification feature has proven to be a powerful security feature, as no-one can forge the biometric and it cannot be stolen. A Personal Identification Number (PIN) can be learned and used to access one's phone. However, with the biometric feature, it is impossible to access the phone without the person being physically present to grant access to the phone. Also, the app itself will ask for the biometric verification, following which the user can use the e-government services platform to access government e-services.

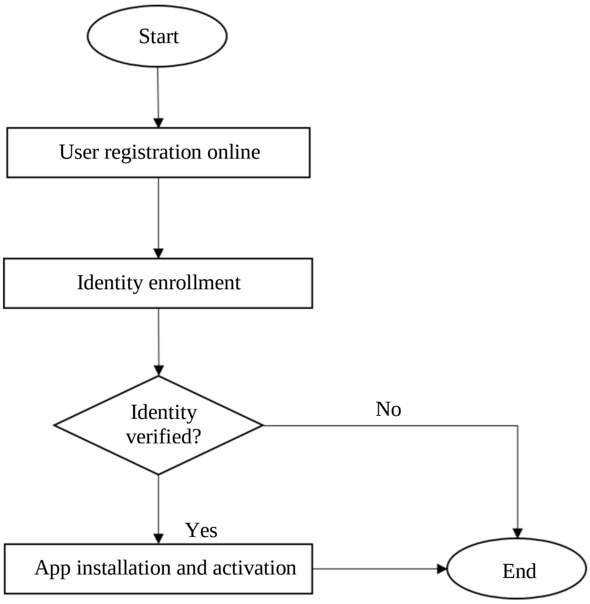

Fig. 2: App-installation process

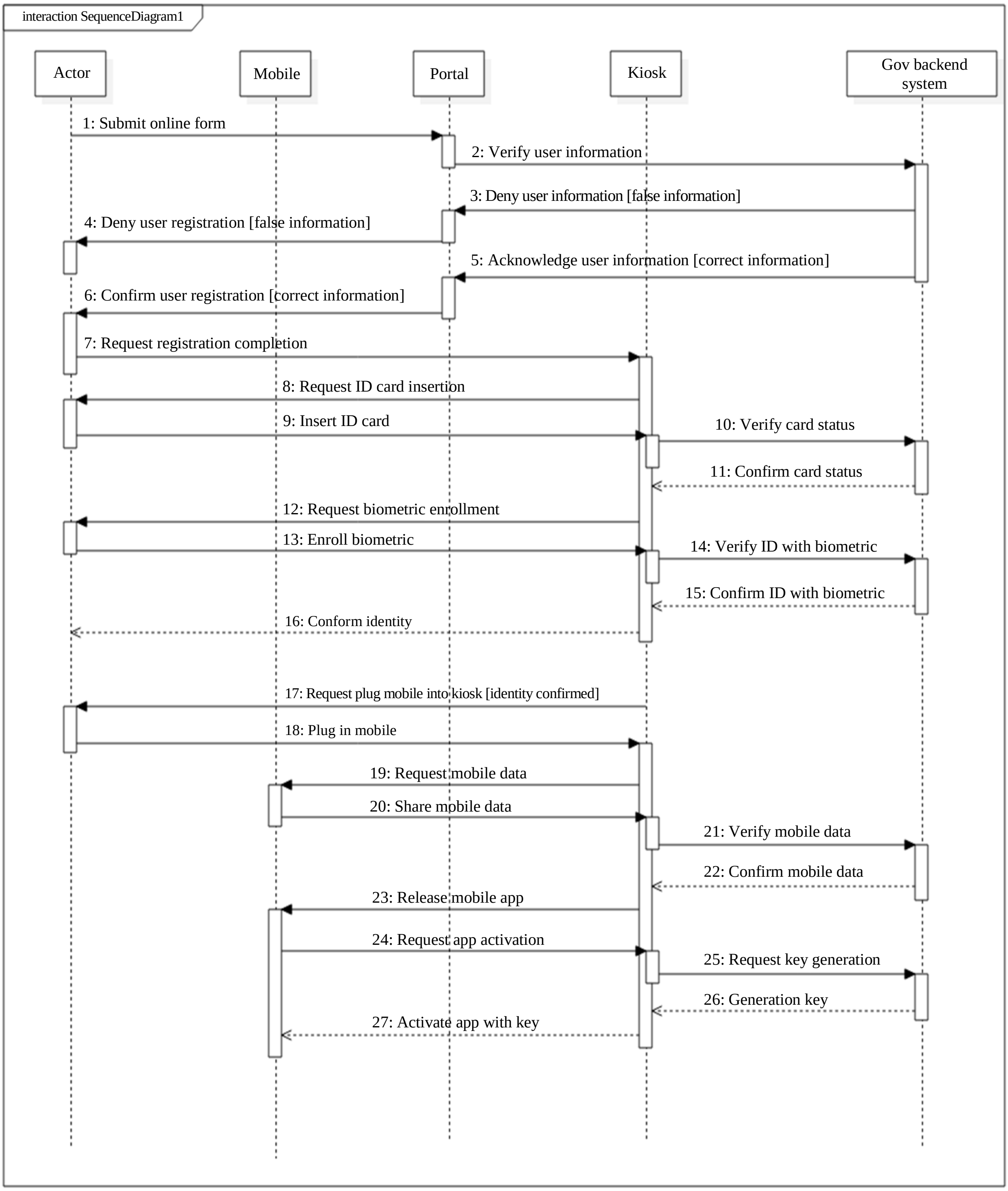
interaction SequenceDiagram1
Actor
Mobile
Portal
Kiosk
Gov backend system
1: Submit online form
2: Verify user information
3: Deny user information [false information]
4: Deny user registration [false information]
5: Acknowledge user information [correct information]
6: Confirm user registration [correct information]
7: Request registration completion
8: Request ID card insertion
9: Insert ID card
10: Verify card status
11: Confirm card status
12: Request biometric enrollment
13: Enroll biometric
14: Verify ID with biometric
15: Confirm ID with biometric
16: Conform identity
17: Request plug mobile into kiosk [identity confirmed]
18: Plug in mobile
19: Request mobile data
20: Share mobile data
21: Verify mobile data
22: Confirm mobile data
23: Release mobile app
24: Request app activation
25: Request key generation
26: Generation key
27: Activate app with key

Fig. 3: Application-installation sequence diagram

The inherent safety and security of the biometric identification system motivated its inclusion in the proposed multi-factor identification model, where users will be required to identify themselves by identifying their biometrics before gaining access to the system. The biometrics and users’ smartphone details will be taken at the kiosks at the governmental Post Offices and users will not be allowed to update them unless they visit the Post Office. Therefore, attackers intending to gain malicious access into the system will not be able to gain access to the system without having the person physically present for confirmation of their biometrics. It is fair to say that the ever-improving technological advances in the smartphone world have enabled the inclusion of biometric-identification the feature into the proposed system.

Users will be forced to use both features, given that both features together are highly secure. Users will have to use the OTP indirectly as well as the biometrics features; if the system detects suspicious activity or logins from unusual locations, then users will be forced to identify their biometrics and the OTP for security purposes.

Conclusion and Future Work

Although the idea behind the conceptual model proposed in this research paper is not new, the real-world application of these ideas is yet to be seen. A major flaw with the current single-factor authentication for e-Government systems is that it lacks the assurance of the user's identity verifications, which represents a significant challenge affecting end-users' privacy and data. Hence, the proposed model has combined different technological security aspects in a way that is advantageous and provides lasting solutions in the ever-expanding technological world. For instance, use of biometrics in the technological world has been around for the past two decades and most industries, especially the banking sector, have implemented the idea as a solution to securing their internal systems and transactions (Della Penna *et al*., 2019, p. 173).

Moreover, many of the newly developed and emerging authentication solutions tend to add more complexity to the user's identity-verifications process for the purposes of users' data protection and security. The proposed conceptual model in this paper presents a simple method with the zero interaction with end users (after the initial set-up) and easy-to-access authentication solutions that can be available through self-service kiosks connected to any government trusted networks, for instant in any Post Office, which will provide users with a seamless, fast, secure and enhanced experience. Accessing the application from trusted networks gives the application security in that potential malicious attackers are not allowed to download the app freely and exploit its code to enable cloning and subsequent attacks on innocent users. Therefore, installing the application only at governmental Post Office kiosks on a secure network increases the security of the model.

Another critical feature the new conceptual model will have over traditional systems is the cost savings and relative ease of operations. In the past, such systems have tended to require users to be furnished with proprietary hardware devices that could generate one-time passwords, which made it impossible for users to access the system without such devices. Users had to travel with these devices in case they needed to access the organization's services.

This model, however, harnesses the power of smartphones and gives them an extra task. As such, the model will save on costs that the government would have accrued in the old system. It also supports users by providing them with extra security features, above what is available in any other solutions that exist in the market and which will allow users to confidently access government services without fear of their data being stolen. Finally, as with any new solution or potential good idea, the users themselves will have the final say on whether this model is useful and acceptable.

Therefore, to build a proof of concept, the author is planning to develop a first prototype of the conceptual model to validate, test and experiment on the model in a real-world case application. This prototype development is left for the future due to lack of time (i.e., the development of a working prototype requires many trial-and-error scenarios before deploying and testing it). Future work concerns developing a prototype and observing and analyzing user experiences, as well as running a deeper analysis of multifactor authentication mechanisms, running security-penetration tests and revising and enhancing the proposed model.

Limitations of the Study

Although the proposed conceptual model promises users a secure authentication solution and a seamless experience, it is important to consider the limitations of this paper and the proposed model.

First, the proposed model is not yet tested; it will require a further investigation in the future to prove the concept, as its planned in future work. Hence, until future investigation has been carried out, the model remains only an idea.

Second, biometric technology is still relatively new, with recent phones implementing this feature to help smartphone users to secure their phones given the increasing importance and influence of phones in people's lives. While only a few phones such as the iPhone had this feature at first, many other smartphone companies have now also included this feature on their phones. The average phone now has biometric identification (facial or fingerprint) as a feature considered as essential as having a camera. This technological leap has allowed the author to use available resources to design a model that offers a multi-factor authentication mechanism that is significantly to previous applications to guarantee the security of the system.

Author's Contributions

Mohammad AlRousan: Contribute to the development of the research and to the writing of the manuscript.

Bendetto Intrigila: Developed the original research idea and contributed in writing the manuscript.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Ashbourn, J., 2014. Biometrics: Advanced Identity Verification: The Complete Guide. 1st Edn., Springer, Berlin, Germany, ISBN-10: 1447107470, pp: 200.

Ashfield, J.M., 2016. Method for using at least a portion of a one-time password as a dynamic card verification value. U.S. Patent 9,251,637 [current assignee: Bank of America Corp].

Bremananth, R. and A. Chitra, 2006. New methodology for a person identification system. Sadhana, 31: 259-276. DOI: 10.1007/BF02703381

Browne, S., 2010. Digital epidermalization: Race, identity and biometrics. Critical Sociol., 36: 131-150. DOI: 10.1177/0896920509347144

Cashell, B., W.D. Jackson, M. Jickling and B. Webel, 2004. The economic impact of cyber-attacks. CRS RL32331. Congressional Research Service, Library of Congress, Washington, USA.

Centeno, C., R. Van Bavel and J.C. Burgelman, 2005. A prospective view of e-government in the European Union. Electronic J. e-Govt., 3: 59-66.

Cisco, 2019. Cisco visual networking index: Global mobile data traffic forecast update, 2017–2022 White Paper. Cisco, San Jose, USA.

Della Penna, G., P. Frasca and B. Intrigila, 2019. Two factor authentication for e-government services using hardware-like one time password generators. J. Comput. Sci., 15: 171-189. DOI: 10.3844/jcssp.2019.171.189

Dmitrienko, A., C. Liebchen, C. Rossow and A.R. Sadeghi, 2014. Security analysis of mobile two-factor authentication schemes. Intel Technol. J., 18: 138-161.

European Commission, 2018. Annex to the commission implementing decision: Laying down the technical specifications regarding the standards for security features and biometrics in passports and travel documents issued by member states and repealing decisions C(2006) 2909 and C(2008) 8657. European Commission, Brussels, Belgium.

Hashizume, K., D.G. Rosado, E. Fernández-Medina and E.B. Fernandez, 2013. An analysis of security issues for cloud computing. J. Internet Services Applic., 4: e5-e5. DOI: 10.1186/1869-0238-4-5

Huang, C.Y., S.P. Ma and K.T. Chen, 2011. Using one-time passwords to prevent password phishing attacks. J. Network Comput. Applic., 34: 1292-1301. DOI: 10.1016/j.jnca.2011.02.004

ICAO, 2015. Machine readable travel documents. International Civil Aviation Organization, Montreal, Canada.

IETF, 1998. A one-time password system. RFC 2289. Internet Engineering Task Force, Fremont, USA.

IETF, 2005. HOTP: An HMAC-based one-time password algorithm. RFC 4226. Internet Engineering Task Force, Fremont, USA.

IETF, 2011. TOTP: Time-based one-time password algorithm. RFC 6238. Internet Engineering Task Force, Fremont, USA.

Law, E.C.W. and L. Yam, 2007. Single one-time password token with single PIN for access to multiple providers. U.S. Patent Application 11/376,771 [current assignee: Boncle Inc].

Leavitt, N., 2011. Mobile security: Finally a serious problem? Computer, 44: 11-14. DOI: 10.1109/MC.2011.184

Mulliner, C., R. Borgaonkar, P. Stewin and J.P. Seifert, 2013. SMS-Based One-Time Passwords: Attacks and Defense. In: Detection of Intrusions and Malware and Vulnerability Assessment, Rieck, K., P. Stewin and J.P. Seifert, (Eds.), Springer, Berlin, Germany, ISBN-13: 978-3-642-39234-4, pp: 150-159.

Nag, A.K., D. Dasgupta and K. Deb, 2014. An adaptive approach for active multi-factor authentication. Proceedings of the 9th Annual Symposium on Information Assurance, Jun. 3-4, Albany, USA.

Stanislav, M., 2015. Two-Factor Authentication. 1st Edn., IT Governance Publishing, Cambridge, UK, ISBN-13: 978-1849287326.

Thirumalai, C. and S. Budugutta, 2018. Public key encryption for SAFE transfer of one time password. Int. J. Pure Applied Math., 118: 283-288.

Velásquez, I., A. Caro and A. Rodríguez, 2018. Kontun: A framework for recommendation of authentication schemes and methods. Inform. Software Technol., 96: 27-37. DOI: 10.1016/j.infsof.2017.11.004

Wang, Y., T. Tan and A.K. Jain, 2003. Combining Face and Iris Biometrics for Identity Verification. In: Audio- and Video-Based Biometric Person Authentication. Kittler, J. and M.S. Nixon (Eds.), Springer, Berlin, Germany, ISBN-10: 978-3-540-40302-9, pp: 805-813.

Weir, C.S., G. Douglas, T. Richardson and M. Jack, 2009. Usable security: User preferences for authentication methods in eBanking and the effects of experience. Interact. Comput., 22: 153-164. DOI: 10.1016/j.intcom.2009.10.001

Yeh, T.C., H.Y. Shen and J.J. Hwang, 2002. A secure one-time password authentication scheme using smart cards. IEICE Trans. Commun., 85: 2515-2518. DOI: 10.1145/1031154.1031164