International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V69I8P205
Volume 69 Issue 8, 36-40, August, 2021

Challenges in Providing Access to Health Facilities for Rural Citizens in Developing Countries

Mohd S M Deris[1,*], Mohamad A Mohamed[2], Rajina R Mohamed[3], Mohd N Derahman[4], Abd R Mamat[5], Mohd F A Kadir[6], Ahmad F A Abidin[7]

[1,2,5,6,7]*Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Besut Campus, Malaysia*

[3]*College of Computer Science and Information Technology, Universiti Tenaga Nasional, Malaysia*

[4]*Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Malaysia*

Abstract *— One of the challenges faced by the IT industry is to provide access to medical care for citizens living in rural areas. Rural areas in some non-developed countries may be physically hardly accessible to the outside world. For that, it will be difficult for those who live in such an area to get access to hospital services. Some illnesses that normally need immediate medical care may end up with fatality to the bearer. In light of this, we survey through the possibility of providing such a virtual appointment in replacement of a physical visit to the rural citizen so that doctors and hospitals can reach out to them. As the basic requirement, the area should have internet coverage, whether wired or wireless. For every household to connect to the application, they need to have a smartphone or computer. As a result, we proposed a simple framework for the online doctor application, which should serve the needs of the public.*

Keywords *— Telemedicine, E-health, Online Doctor, Rural Coverage, Digital Doctor.*

I. INTRODUCTION

In non-developed countries, visiting a doctor in a hospital can be such as depressing task nowadays. In rural areas where hospitals are located far away, with not many clinics available nearby, patients need not only to take a long time to travel but also have to wait in a long queue before seeing a doctor. Not to mention the cost of traveling and consultation, which may be unaffordable and consequently hinder them from getting their illnesses treated. In addition, there are also risks to contracting other's diseases while in the waiting room, even more, harmful to toddlers, babies, and kids. Last year alone, there are almost a billion individual visits to doctors worldwide, and most frequently, these involved non-harmful illnesses such as flu, acne, and coughing. To minimize the said risk, cost and time, we survey into possible telehealth applications which offer easy access to healthcare by allowing a virtual visit to doctors by a patient over the internet at any time and from anywhere.

As reported by the Malaysian Communications and Multimedia Commission, internet coverage in Malaysia has reached 95%, and this becomes the major supportive factor to success. To use the services, patients only need to have a smartphone, connect to the internet, and register to service providers. For a registered patient, a list of doctors will be made available 24x7, ready to serve at the requested time. A patient initiates a consultation request by selecting a doctor and booking the slot if not immediately available. For each consultation, the provider will charge much less than the normal walk-in visits. During the consultation, which will be held through video-conference-like service, two-way communication between patient and doctor takes place to diagnose the disease before the doctor comes out with advice, drug prescription at nearby pharmacies, or recommendation for further treatment in hospital if necessary. To ensure customer's privacy, this application comes with built-in security features, by the use of user authentication technique in addition to encrypted data for all communications.

From a business point of view, the application is expected to attract users from the Malaysian public, corporate, and government agencies. In fact, virtual doctor visit has to become a multi-billion dollar business worldwide, especially in developed countries. Having a good business model, this platform can be commercialized throughout the countries for profits. Most importantly, the success of rolling out this service may be the key point to saving human life by being able to provide immediate access to the citizens who are in need of such care.

In this paper, we examine the challenges and signs of progress of introducing telehealth applications to rural citizens. Section 2 scout through the motivation towards telehealth applications. Section 3 outlay the framework for online doctor consultancy applications. Section 4 dedicates to studying the security of the application in terms of user privacy and authentication. Section 5 concludes the study with some potential future developments.

II. LITERATURE REVIEW

Whether you are at home or in the middle of a road trip, visiting a doctor in walk-in clinics or hospitals can be such as painful task nowadays [1]. In rural areas especially, where hospitals are distant away and with not many clinics available, patients need not only to take a long time to travel but also have to wait in a long queue before seeing a doctor [2-5]. Not to mention the cost of traveling and doctor's consultancy, which may be unaffordable by some villagers and thus hinder them from getting their illness properly treated. In addition, there are also risks to

contracting other's patient diseases while sitting in the waiting room [6], which is even more harmful to toddlers, babies, and kids.

The term telehealth describes the utilization of information, communication and telecommunications technologies to expose and advertise long-distance medical health care, patient and professional health-related education, public health, and health administration [7].

Telehealth brings together patients and doctors much closes in a way access to medical health care is made wider and more reachable. As an alternative approach, telehealth can be seen as a new means to offer patients high-quality and less costly health care. Telehealth services allow patients to access care from their home with only a computer or smartphone to connect with medical specialists via secure video conferencing [8]. In developed countries, telehealth is very rapidly expanding its core services, offering more and more services to the citizens. Health plans may not only come from the same provider but can be provided by a different provider who has expertise and infrastructure in the field. By increasing patient access to providers via virtual technologies, we can improve outcomes while reducing costly and unnecessary visits to hospitals.

Whether to augment existing provider networks, enhance convenience and accessibility for patients, or save time and resources, many health care stakeholders are optimistic about the potential for telehealth to deliver quality, cost-effective care to patients. In developing countries, patients in rural areas, seniors, and others with mobility concerns have experienced the benefits of telehealth, enabling those without immediate access to certain specialty care to receive it through virtual visits.

In the United States alone, in 2016 statistics, there were 1.2 billion patient visits to doctor offices, emergency departments, and hospitals, equivalent to 3.3 visits per US citizen [9]. More than half of those visits involve primary care doctors (prescription refill, coughs, stomach pain, sore throat, earache, and skin rash), of which care can be delivered online. Let say each visit costs $40-$50 [10], which results in a 5 billion dollar business for online doctor consultation.

The concept of virtual doctors has successfully been adopted in the developed countries [11]. In the near future, it is expected that 30-40% of doctor consultations will take place via the internet, and this amounts to $50-60 billion dollars business annually. In developing countries such as Malaysia, the pace is slowly picking up. As reported by MCMC, internet coverage in Malaysia has reached out almost 95% population; this figure shows a good trend in internet usage, and the challenge to introduce virtual doctor visits to the public may be absorbed quickly. With a population of over 30 million, of which 90.7% own a smartphone [12], each of 3.3 visits per year, we have almost 100 million doctor visits in total. Let say each visit costs RM40. If half of the visits can be solved online, it results in 2 billion dollar business annually in online doctor consultation.

III. FRAMEWORK

Nowadays, almost every household owns a smartphone. As long as the coverage reaches them, they will be able to access the internet. In fact, more and more people view their access to the internet as a vital part of their life. The basic requirement of all communication-like applications would be to ensure the application, and the website is easily accessible and highly optimized for mobile devices. This will further encourage citizens with illness to slowly migrate to this coming technology.

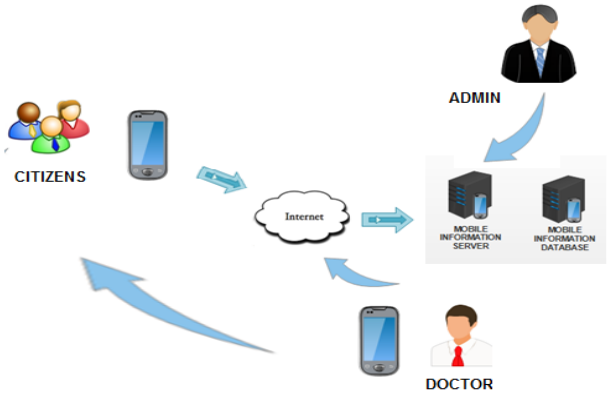

Figure 1: The Framework for Online Doctor Application

In this section, we design the framework suitable for rolling out an online doctor application to the public. Figure 1 shows the basic configuration of our framework with entities such as the administrator, doctors, and citizens as patients communicating via the internet. From the perspective of the entire working environment, each entity will induce its own part of requirements for the system to have. Based on these requirements, each role is assigned different corresponding permissions and actions.

Citizens are spread all over the country, especially into rural areas of which may not have so much accessibility to the government health center. To educate themselves with different diseases and cures, how to identify their symptoms, how and where to get treatment is the first step in minimizing the risk of serious illness or even fatality. This self-care education is very important to the community at large can live with better well-being. With an automatic and digitally recorded and stored, ones' health data can easily be accessible and transferable between authorized parties for better treatment to the patients. Another benefit of e-health would be the capability of providing distant away treatment to those who need it without having to visit the hospital.

For providing the service, the patient can just dial in and have access to a doctor for normal and emergency consultancies, a medical prescription will follow, and drugs can be obtained from the nearby pharmacy. The government doctors must register themselves to the system. It should be accompanied by their medical

knowledge and expertise. Doctors should be able to accept the appointment and treat patients online. On the other hand, the patient should permit the appointed doctor to be able to access her medical history when needed. On top of that, doctors who wish to conduct seminars or workshops to share their health tips and tricks should be able to do so within this platform.

The administrator should be the person who held responsibility for managing and monitoring the smoothness of the operation. Besides, security will also be an important element for an administrator to consider as it could be the cause of huge damage in case of data compromise. For data privacy, the administrator will not be allowed to access a patient's profile, and to ensure the accordance to standard, encryption, and auditing will be enforced. For data confidentiality, end-to-end communication will be encrypted in making sure the message is private to only the chatter. Looking into the aforementioned responsibilities of each entity, we hope to have shed some light on how the virtual doctor visit should look like.

IV. SYSTEM AND SECURITY

The whole system will be developed over an Android platform which leads the operating system market by more than half. It will be supported by the latest technologies such as a one-time password (OTP) and encryption for securing data storage and data communication.

A. Operating System

Android is a Linux-based operating system initially developed by Android.Inc, for touched screen mobile devices such as smartphone and tablet computers [13]. It was initially financially backed and purchased by Google in 2005. Under Open handset Alliance, Android and the team devoted themselves to advancing open standards for mobile devices. The first Android-powered phone was sold in October 2008. Android is open source, and Google releases the code under the Apache License. This open-source and permissive licensing allow the software to be freely modified and distributed by device manufacturers, wireless carriers, and enthusiast developers. Additionally, Android has a large community of developers writing applications that extend the functionality of devices, written primarily in a customized version of the Java programming language. Android platform has been very popular for mobile applications due to several reasons such as ease of use, simple tools, and open-source framework with easily customized and better notification system. Google cloud server is the best choice for offering an online mobile application service due to its robustness and scalability [14].

A. Communication Security

For security purposes, a user authentication technique based on a one-time password (OTP) is a great choice in that it is easy to implement and user-friendly [15]. Data privacy can be achieved using a cryptography algorithm called advanced encryption standard (AES), being the most popular choice [16]. In combination with efficiency, easy to use, and robustness, we embed the security features through OTP and AES techniques.

One-Time-Password (OTP)

A number of different authentication mechanisms are used today in order to alleviate this problem. Enterprise has traditionally used two-factor authentication to secure employee's remote access to corporate resources [17]. A one-time password (OTP) is a suitable candidate for two-factor identification (2FA) and multi-factor authentication (MFA) that satisfies the requirements. An OTP is a unique password to be used only once, with validity limited to a short period of time. Due to non-reusability, OTP managed to overcome weaknesses from within traditional (static) passwords by not being vulnerable to replay attacks. An OTP can be delivered to the user using a few techniques such as soft tokens via a mobile phone app, hard tokens such as key fobs, and on-demand through SMS messages or email. In 2017, FIDO Alliance reported that 21% of businesses utilize soft tokens, 21% use on-demand, while the other 16% use hard tokens.

Software-based OTP solutions cannot guarantee the confidentiality of the generated passwords or even the seed when the mobile OS is compromised. Moreover, they also suffer from denial-of-service attacks when the mobile OS crashes. On the other hand, hardware-based OTP tokens can solve these security problems in the software-based OTP. However, it is inconvenient for the users to carry physical tokens with them. As a result, a new design of secure OTP Tokens using smartphones provides the flexibility of the software tokens and hardware tokens and has been widely used until now [18]. It's also capable of preventing all types of attacks from the malicious mobile OS and can still continue to display the OTP even if the mobile crashes.

Another type of multi-factor OTP authentication is on-demand, used in conjunction with SMS [19]. It uses a one-time password that is communicated to the mobile phone in addition to our user ID and static password to provide an extra layer of high-level security. A user is expected to receive the unique password via text, and it works in combination with a traditional username and password to allow access to a server. Initially, a user needs to register herself to the server. Sometimes before the end, during a few interactions with the server to request the OTP, then a few moments, the user request is received by the server, and then it will be checked, and the user authentication process begins. After approval of the user identity, the server responds to user requests, and the user password requested will code by encryption algorithms and it sent to the user. The user's phone has software in it to decode the received one-time password prior to showing it to the user. The user is expected to type in the OTP in the required space. On the other side, the server processes the OTP, and in this case, if it was rightly input, the user is allowed to log in to the user's page.

Encryption

Modern mathematical-based cryptosystems were drafted following some fundamental principles to ensure their workability in securing the confidentiality of

messages [20]. The original message is encoded as numbers, singly or in groups. Using mathematical functions, these original numbers are transformed into some unintelligible prior to sending over to the receiver. Once received, this crypted message is inverted into an encoded message by reversing the original encryption operation. The encoded message is then decoded back to a readable message. A secure cryptosystem refers to an algorithm which the ability to provide a certain level of security to the encrypted message and to resist some known cryptanalysis attacks. Commonly known as the inability to backward or reverse transform the encrypted message without having the key.

Most of the cryptosystems used nowadays are based on some mathematical structures groups, rings, and field. In general, they can be divided into two categories known as the secret key system and public key system. Secret key system uses the same key for both the encryption of plain messages and the decryption of ciphered messages, and due to this fact, it is only suitable for providing message confidentiality. Data Encryption Standard (DES) cryptosystem was introduced in 1977 by a team at IBM and had been lifted as a standard for more than 20 years. Only recently, Advanced Encryption Standard (AES), which was developed by two Belgium researchers, began to take over DES. Unlike DES, the AES algorithm was made public where its security can be widely studied and scrutinized, and fully trusted by the public.

The public-key system works based on a pair of keys, namely the public key used for encryption and the private key used for decryption of the message. Each party has its own key pair. In order to communicate, the public key of each other must be exchanged a priori. Due to unique keys owned by each party, not only confidentiality but the public-key systems such as RSA [21], El-Gamal [22], and ECC [23] can also warrant authenticity, integrity, and non-repudiation. Although the public-key system is known to be less efficient than the secret-key system, however, it is capable of securing secret key exchange than of secret-key system [24].

Only recently, another breed of cryptosystem based on chaotic functions was purposed. The fact that chaotic function exhibits characteristics comparable to that of mathematical structure qualified for building up cryptosystem. Many physical systems have been identified as being chaotic, while others were intentionally laboratory designed to be chaotic [25-29]. The application of chaos-based cryptosystem was first introduced by Baptista [30], Pecora [31], and Radhwan [32], lately used to secure image communication.

V. CONCLUSIONS

Virtual doctor visit has been proven and well accepted in the developed world, and as the deployment of the necessary infrastructure begins in the developing world, it is expected to offer an affordable primary medical and diagnostic care services to very large populations especially those without physical access. Although the monetary benefits may be about saving billions of dollars (individual, corporation, and government), over time, the greater good may come from saving thousands of lives.

ACKNOWLEDGMENT

This project is funded by the Center for Research Excellence, Incubation Management Center, Universiti Sultan Zainal Abidin, and an internal grant UniSZA/2018/DPU/10.

REFERENCES

[1] Nicolini D. The work to make telemedicine work: a social and articulative view. Soc Sci Med. 62(11) (2006) 2754-67, 2006.

[2] Pal A, Mbarika VW, Cobb-Payton F, Datta P, McCoy S. Telemedicine diffusion in a developing country: the case of India. IEEE Trans Inf Technol Biomed 9(1) (2005) 59-65.

[3] Femi E, Foluso A, Temitope O, Vekima N, Carole D, Victor M, Telemedicine Diffusion in a Developing Country: A Case of Nigeria, Science Journal of Public Health 5(4) (2017) 341-346.

[4] Jetty A, Moore, MA, Coffman M, Petterson S, Bazemore A. Rural Family Physicians Are Twice as Likely to Use Telehealth as Urban Family Physicians. Telemed J E Health 24(4) (2018) 268 - 276.

[5] Smith AC, Bensink M, Armfield N, Stillman J, Caffery L. Telemedicine and Rural Health Care Applications. J Postgrad M 51(2) (2005) 86-93.

[6] Canadian Paediatric Society. Avoiding infection: What to do at the doctor's office. Paediatr Child Health 13(5) (2008) 420–421.

[7] Reed VT, Margo E, Michael LH. Telehealth. The New England Journal of Medicine 377(16) (2017) 1585-1592.

[8] Czaplik M, Bergrath S, Rossaint R, et al. Employment of telemedicine in emergency medicine. Clinical requirement analysis, system development, and first test results. Methods Inf Med. 53(2) (2014) 99 - 107.

[9] Deloitte. eVisits: the 21st-century house call. Available at https://www2.deloitte.com/content/dam/Deloitte/au/Documents/technology-media-telecommunications/deloitte-au-tmt-evisits-011014.pdf

[10] Heidi G. Need an appointment right away? Consider a virtual doctor visit. Harvard Health Publishing. Available at https://www.health.harvard.edu/blog/need-an-appointment-pronto-consider-a-virtual-doctors-visit-2016091610206

[11] Carlo C, Gabriele P, Giuseppe P. Telemedicine for Developing Countries: A Survey and Some Design Issues. Appl Clin Inform 7 (2016) 1025-1050.

[12] Internet Users Survey 2016: Statistical Brief Number Twenty. Malaysian Communications and Multimedia Commission. Available at https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/IUS2016.pdf

[13] Lazare L, Kire J. Analysis of the Advantages and Disadvantages of Android and iOS Systems and Converting Applications from Android to iOS Platform and Vice Versa. American Journal of Software Engineering and Applications 6(5) (2017) 116-120.

[14] Pankaj D K, Gitanjali S. Scalable database management in cloud computing. Procedia Computer Science 70:658-667, (2015).

[15] Khansari N. Kale, G. Survey on one-time password. International Journal of Computer Engineering & Applications. IX(Iii), 1–7.

[16] Ioannis T, Apostolos PF, Nicolas S. Security and Efficiency Analysis of One Time Password. PCI '16 Proceedings of the 20th Pan-Hellenic Conference on Informatics, November (2016) 10-12, Patras, Greece.

[17] Kalaikavitha E, Phil M, Juliana G. Secure Login Using Encrypted One Time Password (OTP) and Mobile Based Login Methodology. International Journal of Engineering and Science 2(10) (2013) 14–17.

[18] Alexander U, Adam B, Colleen H. Advanced Encryption Standard Analysis with Multimedia Data on Intel AES-Ni Architecture. International Journal of Computer Science and Applications 13(2) (2016) 89-105.

[19] Eldefrawy MH, Alghathbar K, Khan MK. OTP-Based Two-Factor Authentication Using Mobile Phones, 2011 Eighth International Conference on Information Technology: New Generations, Las Vegas, NV (2011) 327-331.

[20] Mohamed MA. A survey on elliptic curve cryptography. Applied Mathematical Sciences 8(153-156) (2014) 7665-7691.
[21] Rivest RL, Shamir A, Adlemmaan L. A method for obtaining digital signatures and public-key cryptosystems. Comm. ACM. 21(2) (1978) 120-126.
[22] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Info. Theory 31(4) (1985) 469-472.
[23] Koblitz N. Elliptic curve cryptosystems. Math. Comp. (1987) 48:203-209.
[24] Diffie W, Hellman M. New directions in cryptography. IEEE Trans. Info.Theory 22 (1976) 644-654.
[25] Chlouverakis KE, JC Sprott. Chaotic Hyperjerk Systems. Chaos, Solitons & Fractals 28 (2005) 739–746.
[26] Sambas A, Mamat M, Arafa AA, Mahmoud GM, Mohamed MA, Sanjaya WSM. A new chaotic system with line of equilibria: Dynamics, passive control, and circuit design. International Journal of Electrical and Computer Engineering 9(4) (2019) 2336-2345.
[27] Pehlivan I, Uyaroglu Y. A new chaotic attractor from general Lorenz system family and its electronic experimental implementation. Turk J Elec Eng & Comp Sci 18(2)(2010) 171-184.
[28] Vaidyanathan S, Sambas A, Mohamed MA, Mamat M, Sanjaya WSM. A new hyperchaotic hyperjerk system with three nonlinear terms, its synchronization, and circuit simulation. International Journal of Engineering and Technology(UAE) 7(3) (2018) 1585-1592.
[29] Vaidyanathan S, King ST, Sambas A, Mohamed MA, Mamat M. A new chaotic jerk system with three nonlinearities and synchronization via adaptive backstepping control. International Journal of Engineering and Technology(UAE) 7(3) (2018) 1936-1943.
[30] Baptista MS. Cryptography with chaos. Physics Letters A 240(1-2) (1998) 50-54.
[31] Pecora LM, Carroll TL. Synchronization in chaotic systems. Phys. Rev. Lett. 64 (1990) 821-825.
[32] Radwan AG, AbdElHaleem S H, Abd-El-Hafiz S K. Symmetric encryption algorithms using chaotic and non-chaotic generators: A review. Journal of Advanced Research 7(2) (2016) 193-208.