Development of mHealth Application for Pregnancy Care and Triage

Ravindra Gaikawad (B. E. Comp)
Department of Computer Engineering
Jaihind College of Engineering
Pune, Maharashtra, India

Neha Lonkar (B. E. Comp)
Department of Computer Engineering
Jaihind College of Engineering
Pune, Maharashtra, India

Prashant Said (B. E. Comp)
Department of Computer Engineering
Jaihind College of Engineering
Pune, Maharashtra, India

***Abstract* – The Development Of mobile application for diagnosis and treatment of the pregnant women suffering from many general and serious health problems is described. This application is being developed focusing on the health problems occurring in the low and middle income countries, where the health facilities are not well developed and easily available. The patient or the pregnant woman who will use this application is able to predict the disease. The clinical data will be collected from the patient and the disease is prediction is done on the basis of her primary information as well as the symptoms entered by her. The unique feature of this application is that the patient is monitored remotely by her prescribed doctor. She can generate her own health report. The application will enable the patient to send the health report to doctor and he can use this data to diagnose the patient.**

Keywords: Blowfish, cryptanalysis, mHealth, pre-eclampsia, remote monitoring, risk score, smartphone, triage.

I. INTRODUCTION

In the today's ever growing world, the people are running to catch current scenarios as well as each and every aspect they are required. But in all this daily work they are losing their physical and mental health .So they require health services but these services are based on the working procedure. The most important and essential services are differentiated on the basis of type patient. E.g. woman, children, older person, etc. Because women and children are treated more specially and delicately than other type of patient. As discussed earlier, the health problems are the main issues in the low and middle income countries like India. The health services and facilities are not readily available to people. To overcome this situation in 2008 mHealth alliance was established. The main aim of that to provide the health services in low and middle income countries by using mobile technologies. According to the analyst firm Berg Insight, around 2.8 million patients worldwide were using a home monitoring service based on equipment with integrated connectivity at the end of 2012

In the low and middle income countries the death rate is more due to delay in services, delay in triage, unavailability of medical guidance, etc as compared to the developed countries like U.S. and U.K.[1] To decrease the death rate, the healthcare providers are focusing on the pregnant women and children. Despite the large number of healthcare apps are developed, the majority has only simple functionality; however mobile apps can be used for remote monitoring providing potential for extra data collection to aid healthcare management.[1]

The existing system of this paper is only developed for diagnosis and treatment of pre-eclampsia disease occurred during pregnancy. In this paper we are being eliminating the observed drawbacks and limitations of existing system.

This paper also describes the future work stated by the existing system. This will include a full health record for women during pregnancy.

II. LITERATURE SURVEY

A. Introduction To mHealth

mHealth, which is also written as m-health is an abbreviation for mobile health. This term is used for the practice of medicine and public health supported by mobile devices. The term is most commonly used in reference to using mobile communication devices, such as mobile phones, tablet computers and PDAs, for health services and information. The mHealth field is emerging as a one of the part of health, the use of information and communication technology (ICT), such as computers, mobile phones, communications satellite, patient monitors, etc., for health services and information. mHealth applications mainly uses the mobile devices in collecting community and clinical health data, delivery of healthcare information to practitioners, researchers, and patients, real-time monitoring of patient vital signs, and direct provision of care (via mobile telemedicine).

While mHealth certainly has application for developed and industrialized nations, but the field has emerged in last few years as an application for developing countries, stemming from the rapid rise of mobile phone penetration in low-income nations. The field provides greater access to large portion of a population in developing countries and low and middle income countries, as well as improving the capacity of health systems in such countries to provide quality healthcare. In the mHealth sector, projects operate with a variety of goals, which includes increased access to healthcare and health-related information; improved capacity to diagnose and track diseases and disorders; up to date and more actionable public health information; and extended access to ongoing medical education and training for health workers.

As discussed earlier, At the end of 2012 about 2.8 million patients worldwide were using a home monitoring service based on equipment with integrated connectivity. The figure only includes systems that depends on monitors with integrated connectivity or systems that use monitoring hubs with integrated cellular or fixed-line modems. It is forecasted by Berg Insight that the number of home monitoring systems with integrated communication capabilities will grow at a compound annual growth rate (CAGR) of 26.9 percent between 2011 and 2017 reaching 9.4 million connections globally by the end of the forecast period. The number of these devices that have integrated cellular connectivity increased from 0.73 million in 2011 to about 1.03 million in 2012, and is projected to grow at a CAGR of 46.3 percent to 7.10 million in 2017.

A growing percentage of health-related smartphone apps are available, and some estimates predict 500 million patients will be using such apps at the end of the year 2015.

B. Healthcare And mHealth In LMIC

Low and middle income countries face the constraints in their healthcare systems. These countries face a unavailability of human and physical resources, as well as some of the largest burdens of disease. Poverty is also the main issue in such countries co existing with growing large population with high growth rates. That's why; healthcare access is generally low in these countries. As per the report of WHO higher-income countries show more mHealth activity than lower-income countries. Comparatively, countries in the European Region are currently the most active than other countries and those in the African Region are less active. The WHO observes critical healthcare workforce shortages in about 57 countries—most of which are developing countries and a global deficit of 2.4 million practitioners, nurses, and midwives. The WHO, while studying the healthcare workforce in 12 countries from African region, finds an average density of physicians, nurses and midwives per 1000 population of 0.64. This density is four times as less in the United States, at 2.6.

The burden of disease is much higher in low- and middle-income countries than high-income countries. These burden is measured in disability-adjusted life year (DALY), which is a gap between current health status and an ideal situation where everyone lives into old age, free of disease and disability, is about five times higher in Africa than in high-income countries. In addition, low- and middle-income countries are forced to face the burdens of both extreme poverty and the growing incidence of chronic diseases, such as diabetes and heart disease.

C. Preference To Smartphones

More advanced and developed mobile phone technologies are now enabling the ability for further healthcare delivery. Smartphone technologies are now not only in the hands of handful people but it in the hands of a common man to the large number of physicians and other healthcare workers in low- and middle-income countries. The spread of Smartphone technologies opens up doors for mHealth projects such as technology-based diagnosis support, remote diagnostics and telemedicine, web browsing, GPS navigation, access to web-based patient information, post-visit patient surveillance, and decentralized health management information systems (HMIS).[2] This technology is nothing but the bridge between mobile technology and healthcare.

Although acceptance of Smartphone technology by the medical field has grown in low- and middle-income countries, the capabilities of mobile phones in low- and middle-income countries has not reached the sophistication of those in high-income countries. Because of developing nature and poor economy the infrastructure that enables web browsing, GPS navigation, and email through Smartphones is not as well developed in much of the low- and middle-income countries. Increased availability and working efficiency of both voice and data-transfer systems in addition to fast deployment of wireless infrastructure is accelerating the deployment of mobile-enabled health systems and service, worldwide.[3]

III. SYSTEM IMPLEMENTATION

In this project, work of our system is that to eliminate the limitations and drawbacks of existing system as well as to implement the future work stated. We are developing the mHealth application for the pregnant women for diagnosis and management of their health during all stages of pregnancy.[1]

The main drawback of existing system as we observed is that there is no direct or indirect communication between the healthcare providers (Doctors) and patient. i.e. The symptoms and clinical data were collected during home visit which was not patient requirement based, means that data was collected only when the home visitors visit the home. We are eliminating this drawback by providing indirect(remote) communication between patient and doctor by means of this application. The second one drawback is eliminating by developing the application, by considering the patient itself the main user so that she can do her diagnosis and collect data as per her requirement whereas in existing system the main user is home visitors or sometimes nurses.

We also observed the one limitation of the existing system, that the system was only capable to diagnose and manage the women against the pre-eclampsia this limitation is being overcome by providing the support for all major diseases and disorders occurring during pregnancy. The application can also provide health guidelines and suggestions during pregnancy. In other words we can say that it will acts as an artificial doctor or mobile cum doctor for pregnant women.

The future work of existing system is that to keep full health record of pregnant women, which is also being implemented in our application. Whenever the user/ patient collect her data, the data will be saved in relation database. Thus we are totally improving this mHealth application and making it more efficient from top to bottom.

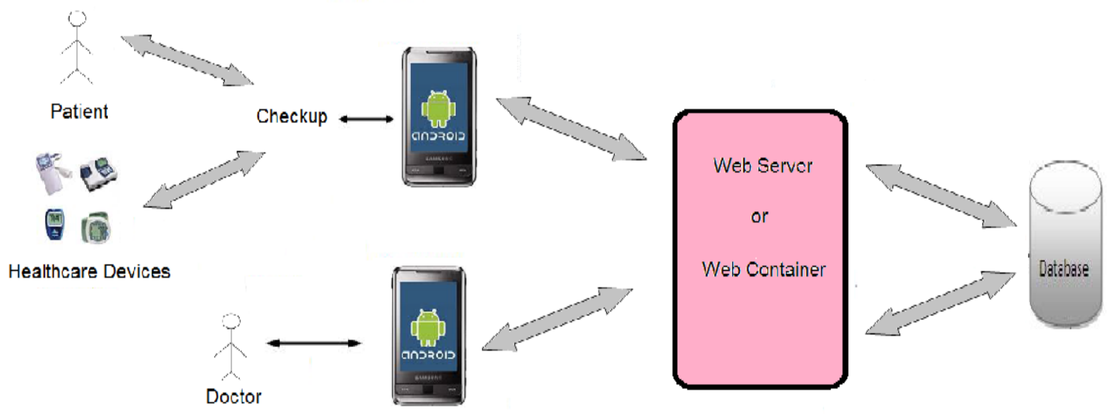

Fig.1 Schematic Architecture of Proposed System

As shown in Fig.1 the proposed system will be Smartphone based, typically it will be android based because in the market the use of android phones are increased beyond the expectation and thinking due to their features.

The patient uses the healthcare devices like pulse oximeter to check and collect reading of blood pressure, heart rate etc. It will also enter the symptoms. then our application will predicts the disease based on the data provided. The proper health solutions will be suggested to patient. The health report is generated and saved in the patients database. The patients can send this report to her prescribed doctor so that doctor can update his database related to patient information and in reply he can provide his suggestions and treatment. Thus patient will monitored remotely.

As the data contained and generated is very sensitive it requires some security provisions. Unlike existing system we are providing user login to application so that only user can itself use the app and handle database. The database also requires security which was provided using blowfish algorithm in existing system, but we are doing this by using the successor of the same algorithm, called as twofish algorithm, a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest. Twofish is related to the earlier block cipher Blowfish.

IV. ALGORITHM

As the data collected during diagnosis is delicate, it should be made secure by using proper data security mechanism. The data should be accessible to authorized one. For this purpose we are using the Blowfish algorithm, a symmetric Feistel cipher using a 128-bit key.[1]
Also in some cases patient i.e. a pregnant woman may want to send her physical samples in the form of images. e.g. images of swollen parts, rashes on belly, some skin infections, etc. The project will have provision for this. The images are taken with the help of built in camera to smartphone. The entire process is generally called as woundcare. But as the images are one of the health related data, may be generated during diagnosis, it should be protected.[2] Therefore these data is also encrypted using blowfish algorithm. The access to the stored data is allowed only through username and password. No effective cryptanalysis has been developed for breaking the full 16-round Blowfish algorithm used in these applications.[1] Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. [9] In structure it resembles CAST-128, which uses fixed S-boxes.

The Fig.2 shows the action of Blowfish. Each line represents 32 bits. The algorithm keeps two subkey arrays: the 18-entry P-array and four 256-entry S-boxes. The input is accepted by S-boxes in 8-bit and produce output 32 bit. One entry of the P-array is used every round, and after the final round, each half of the data block is XORed with one of the two remaining unused P-entries.

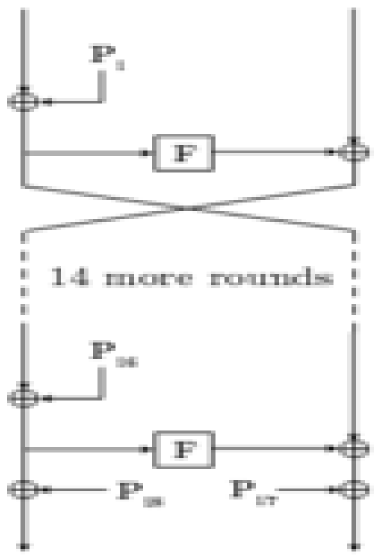

Fig.2 The Feistel structure of Blowfish

Decryption is exactly the reverse procedure as encryption, such that P1, P2,..., P18 are used in the reverse order.[9] This is not so obvious because Xor is commutative and associative. A common misconception is to use inverse order of encryption as decryption algorithm (i.e. first XORing P17 and P18 to the ciphertext block, then using the P-entries in reverse order).

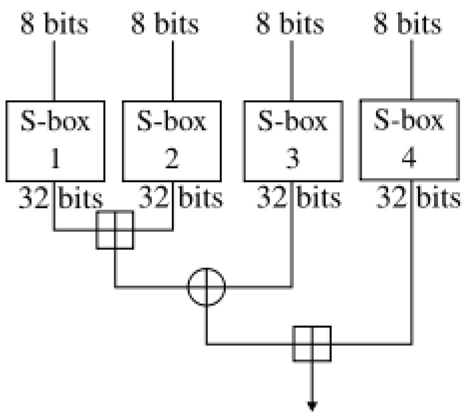

Fig. 3 The round function (Feistel function) of Blowfish

The Fig.3 shows Blowfish's F-function. The function does the job of spliting the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The outputs are added modulo 232 and XORed to produce the final 32-bit output.[2]

Blowfish's key schedule starts by initializing the P-array and S-boxes with values derived from the hexadecimal digits of pi, which contain no obvious pattern. The secret key is then, byte by byte, cycling the key if necessary, XORed with all the P-entries in order. A 64-bit all-zero blocks is then encrypted with the algorithm as it stands. The resultant ciphertext replaces P1 and P2. The same ciphertext is then encrypted again with the new subkeys and the new ciphertext replaces P3 and P4. This continues, replacing the entire P-array and all the S-box entries. In all, the Blowfish encryption algorithm will run 521 times to generate all the subkeys - about 4KB of data is processed. Because the P-array is 576 bits long, and the key bytes are XORed through all these 576 bits during the initialization, many implementations support key sizes up to 576 bits. While this is certainly possible, the 448 bits limit is here to ensure that every bit of every subkey depends on every bit of the key, as the last four values of the P-array don't affect every bit of the ciphertext. This point should be taken in consideration for implementations with a different number of rounds, as even though it increases security against an exhaustive attack, it weakens the security guaranteed by the algorithm. And given the slow initialization of the cipher with each change of key, it is granted a natural protection against brute-force attacks, which doesn't really justify key sizes longer than 448 bits.

V. CONCLUSION

In this paper, we are done a sincere attempt to highlight the limitations and drawbacks of existing system and discussed about our system which is being developed to improve the performance of existing system as well as to eliminate the drawbacks. Proposed system definitely help to peoples to get health services, from low and middle income countries who are suffering from health service related problems. Our system will work as a bridge joining the technical and medical boundary.

ACKNOWLEGEMENT

Foremost, We would like to express our sincere gratitude to our Head of the Department, Mr. Dnyaneshwar Wahval and our guide Ms. Swati Gavale for their continuous support, their patience, motivation, immense knowledge and their complete guidance for this research paper.

REFERENCES

[1] Dustin T. Dunsmuir, Beth A. Payne, Garth Cloete, Christian L. Petersen, Matthias Görges, Joanne Lim, Peter von Dadelszen, et al., “Development of mHealth Applications for Pre-eclampsia Triage”, IEEE Transl., pp. 2168-2194,January 2013

[2] Paul J.F. White, Blake W. Podaima, M.R. Friesen,” Algorithms for Smartphone and tablet image analysis for healthcare applications”, IEEE Transl., pp. 2169-3536,August 2014

[3] Atanu Garai,” Role of mHealth in rural health in India and opportunities for collaboration”, ICCP Technology Foresight Forum: Developments in Mobile Communication, Paris, October 2011

[4] B. Payne, D. Dunsmuir, G. Cloete, G. A. Dumont, D. Hall, J. A. Hutcheon, J. Lim, R. Sikandar, R. Qureshi, E. van Papendorp, M. Ansermino, and P.von Dadelszen, “Re-calibration and improvement of a mobile health decision aid for women with hypertensive disorders of pregnancy in low-resourced settings,” mHealth Summit, Washington, DC, Dec. 8-11, 2013.

[5] K. Thriemer, B. Ley, S. M. Ame, M. K. Puri, R. Hashim, N. Y. Chang, L. A. Salim, R. L. Ochiai, T. F. Wierzba, J. D. Clemens, et al.,“Replacing paper data collection forms with electronic data entry in the field: findings from a study of community-acquired bloodstream infections in Pemba,

Zanzibar," BMC Research Notes, vol. 5, no. 113, 2012

[6] P. von Dadelszen, B. Payne, J. Li, J. M. Ansermino, F. B. Pipkin, A. M.Côté, M. J. Douglas, A. Gruslin, J. A. Hutcheon, K. S. Joseph, et al., "Prediction of adverse maternal outcomes in pre-eclampsia: development and validation of the fullPIERS model," The Lancet, vol. 377, no. 9761, pp. 219-227, 2011.

[7] Vaishnavi B, Yogeshwari R, "A Secured Patient Healthcare Monitoring in Cloud Infrastructure," IJSER, vol.2, issue 1, ISSN 2347-3848, January 2014.

[8] Vikas Agrawal, Shruti Agrawal, Rajesh Deshmukh, "Analysis and Review of Encryption and Decryption for Secure Communication," IJSER, vol.2, issue 2, ISSN 2347-3848, February 2014.

[9] Pia Singh, Karamjit Singh, "Image Encryption and Decryption Using Blowfish Algorithm in Matlab," IJSER, vol.4, issue 7, ISSN 2347-3848, July 2013.