ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Volume 2, Special Issue 19, October 2016

E-Health Security using ECC algorithm

R. Sridevi,
Assistant Professor,
Department of Computer Science,
PSG College of Arts and Science.

C.Nithiya,
Research Scholar,
Department of Computer Science,
PSG College of Arts and Science

***Abstract*-Implementing security in healthcare systems has become a challenge nowadays. Dealing with the privacy of the Patient's health record is very mandatory as failures may lead to much many problems. In this paper we propose a system for taking care of the patient's privacy by building a system that secures the information of patients by implementing ECC algorithm.**

Keywords-ECC, Healthcare, authentication and authorization, public key encryption

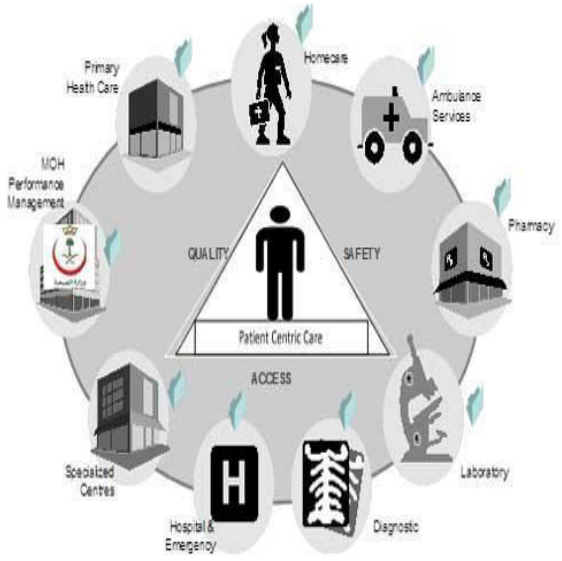
I. INTRODUCTION

The security of health care system is the most needed security implementation. The health record of patients might be under threat. Health care organizations are quickly facing security issues and vulnerabilities through the implementation of digitalization of patient records. The goal of health care systems is to deliver the maximum health service for anyone. Privacy is one of the major factors which have a sub factor in the form of confidentiality which is required to check the revelation of patient's sensitive information. Data security is the most needed and important thing to be considered in any heathcare sector. Improving security deals with increasing confidentiality, securing privacy and avoiding threats. The communication has to be very confidential between the doctor and the patient. The main goals of this system include privacy, integrity and confidentiality. The main purpose of this paper is to propose a secure health care system that might not be attacked by other users. The main aim includes user satisfaction and performance of the system.

II. E-HEALTH

Technology and automation of health care system has the ability to reduce the cost for offering good healthcare treatments. This framework plays a major role in maintaining the security of the healthcare. The WHO defines e-health as 'being leveraging of the information and communication technology to connect provider and patients and governments; to educate and inform healthcare professionals, managers and consumer; to stimulate innovation in care delivery and health system management; and, to improve our healthcare system'. The impact of this healthcare system on the people was high so that people entering a medical organization has various enquiries about the contacts through the internet. The existing system has been extremely helpful to the health and recovery of patients. This healthcare involves major role played by the Information and Communication technologies.

The main goals of the healthcare include Efficiency, Quality, Security, Empowerment of patients, Education of physicians, Ethics and Equity.



III. ADVANTAGES OF E-HEALTH FRAMEWORK

There are many advantages in using E-Health systems. Before E-health came into use, we used records in papers to record patient history. These paper based system might not be very accurate while comparing with the electronic system. Coming to E-health, the data that is stored electronically is more simple and efficient. By using E-health, there are

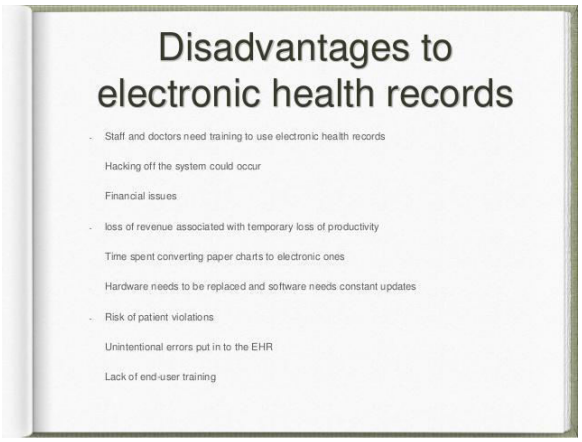
many advantages to different people such as doctors, patients, etc. For example, doctor's orders can be placed by machine, which avoid wrong details of hand written records. And with the help of E-health, most doctors shrink the time of locating and analyze patient health information. To the patient, they can begin to be steadily alert of the importance of self-care management. Moreover, it is also convenient for maintaining only with some experts in medical and application developers.

IV. DISADVANTAGES OF E-HEALTH FRAMEWORK

The following are the main barriers to E-health.

Operational Barriers - This area of concern relates to the interoperability of systems which e-Health aims to provide. First, a system has to be developed with an interface allowing presented computer system to correspond with new system, which e-Health will introduce. Second, there must be a common standard electronic language to cross communicate between different healthcare organization about the medical data, such as patient records and hospital internal record.

Cost/Benefit Barriers - As the name suggest it is the barrier associated to the expenditure in implementing e-Health solutions, whether it is promising in-terms of cost wise i.e. do the profit of e-Health outweigh the cost required to implement E-health. From the technical side, the execution of E-health solutions is clearly advantageous in contrast with past methods such as the paper-based record keeping systems but from the healthcare organization side these benefits may not be more important than the cost of implementing e-Health solutions. The cost of implementing e-Health solutions can be tens of thousands of dollars and this does not even include the obligation of hiring teams of IT professionals to bear and maintain the software throughout its life cycle.



V. ECC ALGORITHM

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. ECC was developed by Certicom, a mobile e-business security provider, and was recently licensed by Hifn, a manufacturer of integrated circuitry (IC) and network security products. RSA has been developing its own version of ECC. The properties and functions of elliptic curves have been studied in mathematics for 150 years. Their use within cryptography was first proposed in 1985, (separately) by Neal Koblitz from the University of Washington, and Victor Miller at IBM. An elliptic curve is not an ellipse (oval shape), but is represented as a looping line intersecting two axes (lines on a graph used to indicate the position of a point). ECC is based on properties of a particular type of equation created from the mathematical group (a set of values for which operations can be performed on any two members of the group to produce a third member) derived from points where the line intersects the axes. Multiplying a point on the curve by a number will produce another point on the curve, but it is very difficult to find what number was used, even if you know the original point and the result. Equations based on elliptic curves have a characteristic that is very valuable for cryptography purposes: they are

relatively easy to perform, and extremely difficult to reverse.

Algorithm 3: *ElGamal elliptic curve encryption*

Input: Parameters field of elliptic curve (p, E, P, n), Public key Q, Plain text m
Output: Cipher text (C_1, C_2)
begin
1. Represent the message m as a point M in E (F_p)
2. Select $k \in R^{[1,n-1]}$.
3. Compute $C_1 = kP$
4. Compute $C_2 = M + kQ$.
5. Return (C_1, C_2)

end

Algorithm 4: *ElGamal elliptic curve decryption*

Entrada: Parameters field of elliptic curve (p, E, P, n), Private key d, Cipher text (C_1, C_2)
Saída: Plain text m
início
1. Compute $M = C_2 - dC_1$, and m from M.
2. Return (m).

fim

A. Computation of Point on the Curve

The security of ECC algorithm depends on its ability to compute a new point on the curve given the product points and encrypt this point as information to be exchanged between the end users.

B. Choice of Field

Although RSA public key cryptosystem is a secure asymmetric-key cryptosystem, its security comes with a price of larger key sizes and computational power. Many researchers have looked for an alternative to this system with a smaller key size while maintaining the same level of security. The ECC system is based on the concepts of Elliptic Curves. To analyze the time taken by an algorithm researches have introduced polynomial time algorithms and exponential time algorithms. Algorithms with smaller computation can be evaluated with polynomial time algorithms and complex computations can be evaluated with exponential time algorithms. The equation of an elliptic curve is given as,

y2 = x3 + ax + b

C. Key Generation

Key generation is an important part where an algorithm should generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key. Now, select a

number, d within the range of n. Generate the public key using the following equation,

Q = d * P

Where d = the random number selected within the range of (1to n-1). P is the point on the curve, Q is the public key and d is the private key.

D. Encryption

Let 'm' be the message that has to be sent. Consider 'm' has the point 'M' on the curve 'E'. Randomly select 'k' from [1 -(n-1)]. Two cipher texts will be generated let it be C1 and C2.

C1 = k * P

C2 = M + (k * P)

E. Decryption

Use the following equation to get back the original message 'm' that was sent.

M = C2 - d * C1

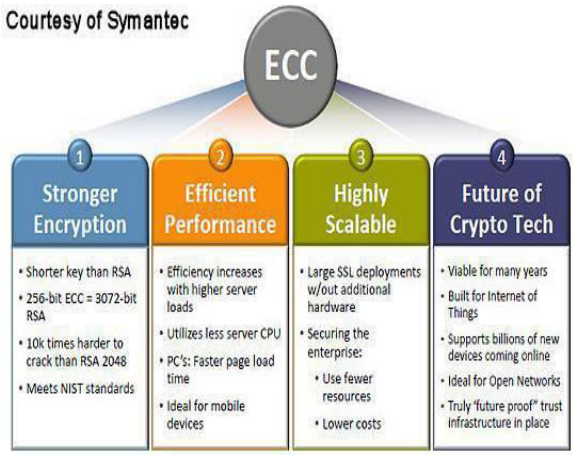
M is the original message that was sent.

VI. ADVANTAGES OF USING ECC ALGORITHM

ECC employs a comparatively short encryption key -- a value that must be fed into the encryption algorithm to decode an encrypted message. This short key is faster and requires less computing power than other first-generation encryption public key algorithms. For example, a 160-bit ECC encryption key provides the same security as a 1024-bit RSA encryption key and can be up to 15 times faster, depending on the platform on which it is implemented. RSA is a first-generation public-key cryptography technique invented by Ronald Rivest, Adi Shamir and Leonard Adleman in the late 70s. Both RSA and ECC are in widespread use. The advantages of ECC over RSA are particularly important in wireless devices, where computing power, memory and battery life are limited.

Main benefits of using cryptographic algorithms based on elliptic curves rather than cryptographic algorithms based on finite fields, such as RSA or DSA include a smaller size of key for security equivalence, the possibility to implement without

crypto processor, and the faster execution in some cases when using a crypto processor.



CONCLUSION

The E-Health framework aims to record the patient information without having any compromise towards the security of data. Since ECC algorithm is used, the key size is considered to be a great advantage. The performance of the system is another advantage to be considered while using ECC. This framework might be useful for the patients who cannot attend regular checkup and can contact the physicians. When the patient has to get an opinion from another consultant also the records of the patient stored in this system can be shown with the access by the patient.

REFERENCES

1. _http://www.globdev.org/files/9-Paper-Li-E- Health-Readiness-Revised.PDF
2. http://people.ischool.berkeley.edu/~glushko/ISE-Notes-Fall2006/E-HealthPreparedness.pdf
3. http://eujournal.org/index.php/esj/article/view/6014
4. http://ijcsit.com/docs/Volume%206/vol6issue04/ijcsit2015060472.pdf
5. http://s3.amazonaws.com/academia.edu.documents/46412360/Enhanced_e-Health_Framework_for_Security_and_Privacy_in_Healthcare_System_1.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMTNPEA&Expires=1474263976&Signature=HSGORcHOIZjKSvzu7F6GFq88M9w%3D&response-content-disposition=inline%3B%20filename%3DEnhanced_e-Health_Framework_for_Security.pdf
6. L. Barua, & Shen, "Secure Personal Health Information Sharing," Symposium of Communication and Information System Security, pp. 201-205, 2013
7. P. Mehndiratta, " A Model of Privacy and Security for Electronic Health Records," A Model of Privacy and Security for Electronic Health Records," In Bhalla Springer International Conference, pp. 202-213, 2014.