International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 03 | Mar -2020 ISSN: 2582-3930

Authentication Using Elliptical Curve Cryptography for e-Healthcare System

V.P.Gaikwad [Assistant Professor, Computer Science Department, Priyadarshini Bhagawati College of Engineering] 28/02/2020

Rutuja Somkuwar [CSE P.B.C.O.E Nagpur, Maharashtra, India] **28/02/2020**

Mrunali Barde [CSE P.B.C.O.E Nagpur, Maharashtra, India] **28/02/2020** Jagruti

Burde [CSE P.B.C.O.E Nagpur, Maharashtra, India] **28/02/2020** Tejaswini

Vaidya [CSE P.B.C.O.E Nagpur, Maharashtra, India] **28/02/2020**

Abstract

Medical record's security attracts a lot of attention these days. Whatever the security of health care improves, its application becomes wider. Li et al. marked this issue by proposing a new privacy preserving RFID authentication protocol for e-health care.[1]

Health care is one among the major sectors, where we concentrate more and spend lot of time to increase our services to the doctors and patients. Today many health care departments are giving free treatment and medicine to get more popular. In order to monitor the incoming out going patients the application has been designed with a real time implementation. To maintain the privacy the data are stored in the cloud server with a private and public key using cryptographic technique. The application has an

1. Introduction

Medical services are rapidly increasing and thus quality of health care is critical. Via the Internet, patients will send or access health data and use portals for health observance and healthcare-related services. Gradual development of health care systems from table work to wireless and mobile platforms brings down medical services directly into the patient's home, affiliation is established between patient and doctor with economical alternatives for each patients and healthcare service suppliers. This can decrease the travel expense and increase productive time, comprehensive higher cognitive process and improved patient compliance.

Electronic medical history square measure hold on in servers which may give various services to users, physicians, hospitals, health care organizations medical servers will authenticate users, physicians update database and will monitor exchange of data packets patient's privacy will ensured at all levels. Encryption of all sensitive information related patient's health will be ensured medical system. Illegal user cannot access the authenticated scheme. Recent authentication schemes are password based. Unavoidable attacks such as dictionary attacks, desynchronization attacks, replay attacks, etc., are bridled by two factor authentication schemes where the user sends id and password in ordered to get authenticated during login phase. Id and password are issued by system during registration phase access to various facilities are granted by administration.

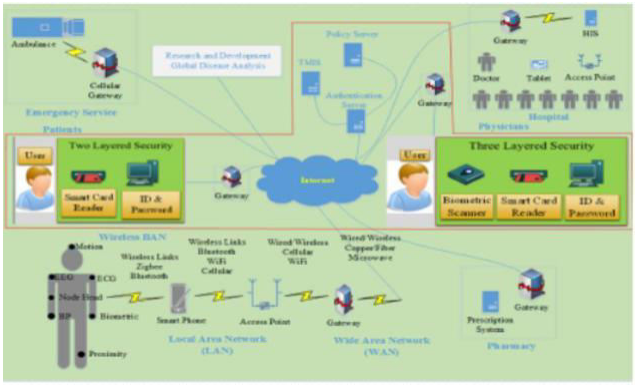

Figure1: e-Healthcare architecture [2]

1.1 ELLIPTIC CURVE CRYPTOGRAPHY [ECC]

Elliptic curve cryptography is a public key cryptography built on algebraic structure of elliptic curve atop finite fields. ECC has smaller key compare to other algorithms which provide coequal security. ECC is apt for key agreement digital signature, pseudo-random generators and other chores. Symmetric encryption is none by heckling the key agreement. Elliptic curve is a plain curve over a finite field by merging points satisfying the equation

= + + , along a determined points at infinite.

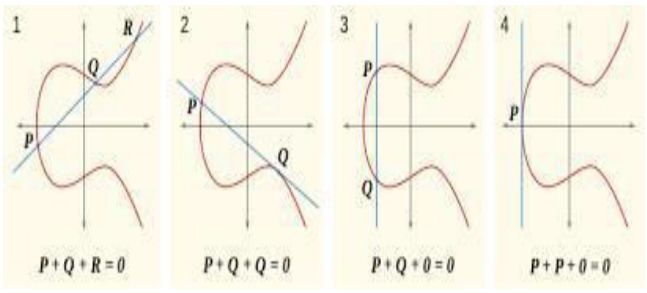

Figure2 : Elliptic Curve

1.2 Basic Concepts

Elliptic Curve Cryptography can be explained by plotting a graph on X and Y axis.
Graph is symmetric about X-axis. If we draw straight line through curve it will hit curve at multiple points.

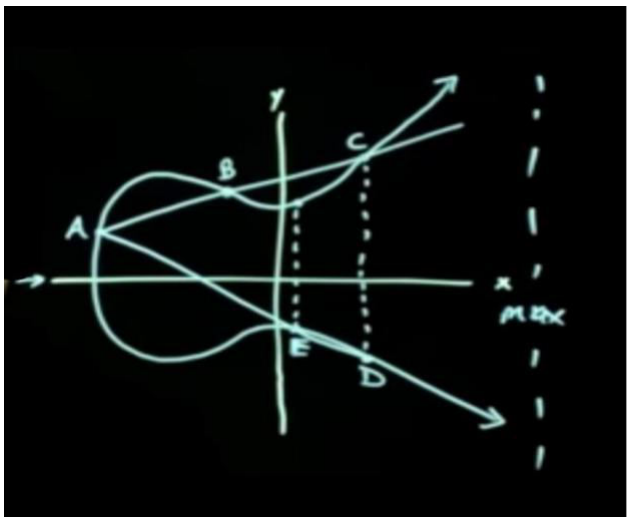

Figure3: Demonstration of ECC

Dotting of graph can be denoted as A dot B → C. It can be dotted n times yielding multiple values. For this we have to set maximum point (let m). If we do this function over and over and if the value goes beyond the maximum limit you have to bring it back to beginning.

The goal is to keep everything within the maximum limit m.

In public key cryptography , the key size can be equal to maximum value . If you are given this curve the starting and ending points, when asked to dot itself it turns out to be extremely difficult to find out the number of times you dotted to get that point.

This makes it liable to give out public information and still keep data private.

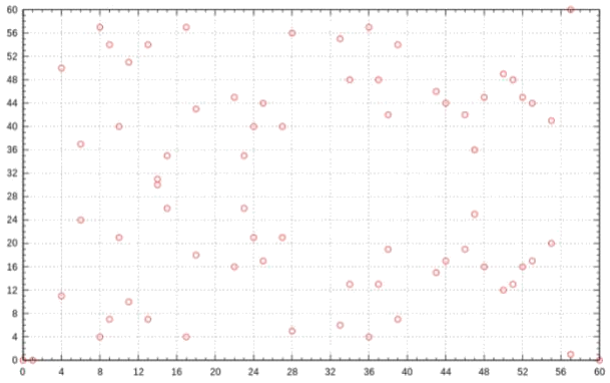

Figure 3 : Elliptic Curve over Finite prime fields [3]

2. Related Works

In the field of health care, the privacy of the user and also the security of their information could be a terribly vital issue. The user may be a doctor, a nurse or a patient and their info may vary from their personal information to the history of their medical services then on. Plenty of steps or taken within the direction of e-health care system however still, a restricted work is found with relevance it. New technologies, like RFID will improve the standard and therefore the speed of the medical services that is gived for suppliers to supply higher service for his or her patients . Rathar than it new technologies has their own risks and considerations misappropriated access to the system info could be a risk which might cause several issuess varies from compromising the user's privacy to grant wrong medical service to a patient that cause to his/her death. Its been known many existing authentication schemes or liable to several weakness and lots of such schemes don't give watchword recovery phases.

In the recent years, there are several echt protocols e-Healthcare system. Li et al. noticed the protection vulnerabilities as well as having a weak login section that will increase the adversary's advantage to a prosperous login, its weakness against the stolen/lost reader and additionally having low potency. Amin et al. introduced a password recovery section, which might be committed if user forgets his password. Amin et al.'s multniserver scheme is liable to many weakness as well as stolen smart card and stolen verifier attack. Zhou et al. [1] showed weaknesses of Li et al. protocol and proposed a protocol, used residue theorem and additionally hash functions as building blocks of their planned proposal and claimed to be appropriate for TMIS applications. Mir and Nikooghamdam tried to use biometric in their authentication with ey agreement protocol for TMIS. Liu et al. planned a certificate less signature (CLS) scheme ad used it to style 2 certificate less remote anonymous authentication schemes for telecare system. Islam et al. planned a 2 issue authentication protocol, that is applicable for the integrated electronic patient information data system. Srivastava et al. planned a hash-based mutual RFID authentication protocol in Telecare Medicine Information System (TMIS) and claimed security against active and passive attacks such as forgery, traceability, replay and desynchronizing attack. What is more wazid et al. designed a 3 factor authentication and key agreement framework with obscurity preservation for care system. Benssalah et al. showed protocol as well as vulnerability against desynchronizing associate degreed impersonation attacks and additionally not guaranteeing the protocol's transferred messages integrity and additionally information privacy and additionally planned an improved version. Sutrala et al.advised a secure RSA assisted authentication protocol with patient obscurity for TMIS and their protocol is secure via correct security investigation and verification tool.

3. Proposed System

Proposed authentication scheme involves four bodies: patient, server, doctor, health care center comprising of four phases, namely

1. Health care center's
2. Patient's
3. Treatment
4. Examination

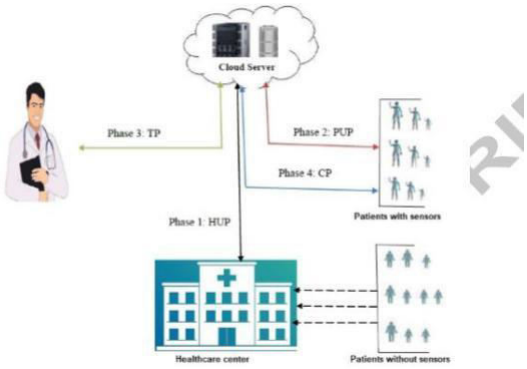

Figure 4: Architecture of proposed protocol with different phases. [2]

Data from local device is uploaded to dedicated server in each phase. The description of each phase is explained as follows.

1. Health care center's:

Patient will register at hospital and it will provide unique ID to Patient. The verification process will be operated by hospital with the help of server and sends the patient's inspected medical data back to server.

2. Patient's:

Patient visiting for the first time will have to register themselves with any of the healthcare center. Once they register, their data will be inspected and stored safely into the server. The patient's health information now can be used by the doctor for further medication of the patient.

3. Treatment:

In this phase, doctor provides the treatment to patient. The server will have all the inspected data of further treatment.

4. Examination:

After completion of the treatment phase, the doctor can download the inspected medical report from the server. Through mobile safely device the patient can access the prescribed medicine and can take the medication. Even the doctor can easily access the patient's data and can track the medical state.

3.1 Working

Three user patient, doctor and server will have to register and will get credentials. All the data will be stored into the server.

They have to authenticate themselves as a verified user. Authentication will be done in **Two Phase Protocol** which includes

1. Password
2. OTP

Password will be set by user through themselves and OTP will be sent on user's verified email id or through contact number.

Functioning of each user

i. Patient: Once a patient gets registered, they will have to fill their personal information, medical history and allergies(if any).
Each time the patient logins they will have access to fill-in their current medical condition and will be able to post query.
Medicines prescribed by the physician can only be read by patient.

ii. Doctor: Doctor will register themselves with there respective healthcare centers. All their personal detail will be available with the hospital and will be saved in the server. Doctors could read patient's medical history and give them prescription.
Both patient and doctor will be unaware of server.

iii. Server: Server will be managed by health care center and will be able to access doctor's and patient's data.

Each time patient or doctor will try to access the server they will have to authenticate themself. Date stored/ retrieved from the server will be in ciphered form. Transfer of data between doctor/patient and server is being testified by ECC authentication algorithm.

4. Future Scope

Adding to our proposed system, an hybrid algorithm can be applied. The SMS services can be purchased by Telecom Service Providers. Pretty Good Privacy (PGP) available with top email service holder can be used to increase security notches. By collaborating with mobile companies and adding in-built sensors the system can be Three Factor Authenticated.

5. Conclusion

In this system, the proposed authentication scheme uses algebraic values of elliptic curves to achieve data privacy. Furthermore it is evitable that security is a myth and it's ability to withstand against attacks requires high cost and will add-on complexity.

References

1. Masoumeh Safkhani and Athanasios Vasilakos, A new secure authentication protocol for telecare medicine information system and smart campus. In: *Digital Object Identifier*,2019
2. Muhammad Umair Aslam, Abdelouahid Derhab, Kashif Saleem . A survey of authentication schemes in telecare medicine information systems. In: *Springer Science+Business Media*, 2016
3. Iskandar Setiadi, Elliptic Curve Cryptography: Algorithm s and Implementation Analysis over Coordinate Systems .In : https://www.researchgate.net/publication/268688957,2014