International Conference on Advances in Materials, Computing and Communication Technologies
In Association with International Journal of Scientific Research in Science and Technology
Volume 9 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)

Security for EHR Based on ECC with Reconstruction Method

Benil T[1], Berlin Shaheema S[2], Jasper J[3]

[1]Department of Computer Science and Engineering, Ponjesly College of Engineering, Nagercoil, Tamil Nadu, India

[2]Department of Computer Science and Engineering, Annai Vailankanni College of Engineering, Nagercoil, Tamil Nadu, India

[3]Department of Electrical and Electronics Engineering, Ponjesly College of Engineering, Nagercoil, Tamil Nadu, India

ABSTRACT

Electronic Health Record plays vital role in hospitals and healthcare organizations. security is one of the main issues in EHR . Electronic Health Record allows only the licensed people can access the records. EHR ensure high-quality care. EHR contain treatment histories of patients. Using basic algorithms like symmetric algorithms, public key cryptography, RSA algorithm the Electronic health care can be secured, but there may be a few drawbacks to obtain integrity and confidentiality .The proposed ECC (Elliptical Curve Cryptography) will provide high security in EHR and obtain confidentiality and integrity. The doctors diagnoses, treatment plans, radiology images, and laboratory a test results. Treatments and guidance from doctors to patients mostly through e-mails, also many parties store and run computation while keeping the sensitive health data private.so cipher attack may cause heavy damage from the patients side therefore data may be secure. In order to address this issue this paper presents a patient healthcare data management system using reconstruction outsourcing mechanism to attain privacy in HC.

Keywords - Electronic Health Record, Symmetric key, ECC, HealthCare.

I. INTRODUCTION

Cryptography has been in use for centuries now, and the earliest ciphers were either used transposition or substitution, and messages were encoded and decoded by hand. However, these schemes satisfied only the basic requirement of confidentiality. In more recent times, with the invention of processing machines, more robust algorithms were required, as the simple ciphers were easy to decode using these machines, and moreover they did not have any of the afore mentioned properties. Secure data communication became a necessity in the 20t h century and a lot of research was done in this field by government agencies, during and following the world-wars. The most famous machine of this time.

An electronic health record (EHR) is a digital version of a records maintenance systems in hospitals and healthcare organizations. EHRs allows only the

licensed people can access the records. HER contain treatment histories of patients, ,doctors diagnoses, treatment plans, radiology images, and laboratory a test results. EHR allow doctors to know about the patient's medical history and the health of the patients .Doctors or authorized persons can access the EHR data's from anywhere in the world through cloud-based-HER- Systems (CBES). One of the key features of an EHR is that patient's health information can be created and managed by licensed providers in a digital format through wallet or smart devices.

II. HISTORY

II.1 Symmetric Algorithms

The first secret key-based cryptographic algorithms worked on the symmetric algorithms. They assumed that both communicating parties shared some secret information, which was unique to them, much like the older One Time Pads. Using this secret information, also called a key, the sender encrypted the data, and the recipient was able to decrypt.

II.2 Public Key cryptography

The concept of Public Key cryptography (PKC) was first introduced by Di e and Hellman in 1976, in their seminal paper, New Directions in Cryptography [DH76]. This paper also addressed the issue of key exchange, based on the intractability of the discrete logarithm problem. In a public key cryptosystem, each user has a pair of keys, one published publicly, known as the public key, and the other known as a private key, is stored in a secure location. Public key cryptosystems rely on the existence of a trapdoor function, which makes decoding possible given the knowledge of the private key corresponding to the public key for encryption.

III. CURRENT TECHNOLOGY – RSA

RSA stands for Rivest, Adleman and Shamir, who devised this algorithm in 1977 at MIT. RSA is the most widely used public-key encryption scheme today. The US patent on the RSA algorithm expired in 2000, but as the algorithm was already published prior to patent application, it precluded patents elsewhere. The security of the RSA cryptosystem is based on two mathematical problems: the problem of factoring very large numbers, and the RSA problem. Both of these problems are hard, i.e., no e client algorithm exists for solving them. The RSA problem is defined as the task of taking eth roots modulo a composite n: recovering a value m such that me = c (mod n), where (e, n) is the public key and c is the cipher text. Currently the most promising approach to solving the RSA problem is to factor the modulus n. With the ability to recover prime factors, an attacker can compute the secret exponent d from a public key (e, n), then decrypt c using the standard procedure. To accomplish this, an attacker factors n into p and q, and computes (p–1)(q–1) which allows the determination of d from e. No polynomial-time method for factoring large integers on a classical computer has yet been found.

III.1 ECC

Elliptic Curve Cryptography is an approach to public-key cryptography, based on elliptic curves over finite fields. The technique was first proposed individually by Neal Koblitz and Victor Miller in 1985. The ECC is based on the Elliptic Curve Discrete Logarithm problem, which is a known NP- Hard problem. An elliptic curve is defined by the equation,

$y2 + xy = x3 + ax + b$†

Operations on Elliptic Curves

The crucial property of an elliptic curve is that we can define a rule for adding two points which are on the

curve, to obtain a third point which is also on the curve. This addition rule satisfies the normal properties of addition. The points and the addition law form a finite Abelian group.[Bar97] For addition to be well defined for any two points, we need to include an extra zero point 0, which does not satisfy the elliptic curve equation. 0 is taken to be a point of the curve. The order of the curve is the number of distinct points on the curve, including the zero point. Having defined addition of two points, we can also define multiplication kP where k is a positive integer and P is a point as the sum of k copies of P.

The main advantage ECC has over RSA is that the basic operation in ECC is point addition which is known to be computationally very expensive. This is one of the reasons why it is very unlikely that a general sub-exponential attack on ECC will be discovered in the near future, though ECC has a few attacks on a few particular classes of curves. These curves can be readily distinguished and can be avoided. On the other hand, RSA already has a known sub-exponential attack which works in general. Thus, to maintain the same degree of security, in view of rising computing power, the number of bits required in the RSA generated key pair will rise much faster than in the ECC generated key pair malpractices is based on the correctness and timeliness of EHRs.

IV. RELATED WORK

Users, individuals and medical institutions consider a flexible way to manage their EHRs. Since EHRs are most sensitive and it contain patients confidential data's, cloud-assisted eHealth systems also suffer from challenging privacy and security threats toward outsourced EHRs. To protect patients' privacy against internal adversaries and external adversaries, EHRs are encrypted before outsourcing. Few papers proposed a cryptographic key management solution for protection of patients' EHRs. However, this scheme employs a trusted server to process all secret keys of patients. As a consequence, the trusted server is able to retrieve the patients' EHRs, and the privacy of patients is not well protected. Many paper proposed a secure EHR system to protect patients' privacy without introducing any trusted entity. The system model of this scheme is not permanent with current cloud-assisted systems. The above two schemes, patients' EHRs are outsourced by the patients themselves, and before outsourcing the doctor needs to send EHRs to the patients .This brings heavy burden in terms of communication and computation costs. In recent studies says that the integrity of outsourced data has also attracted. These schemes mainly focus on ensuring that the outsourced data would not be lost, and the data owners generate and outsource the data to the cloud server, the doctor is only trusted during the treatment period, if the malicious doctor incentivizes the cloud server to tamper with outsourced EHRs generated by himself, it is hard to detect such misbehaviour. Moreover, existing schemes do not consider the timeliness of EHRs. We stress that it is also important to know when EHRs were generated in eHealth systems, since the correctness and fairness of conclusions drawn from EHRs in judgements and dispute resolutions in medical

V. PROPOSED METHOD

The proposed cloud storage scheme for EHRs consists of four phases, namely the Data Processing phase, the issuing phase, the reconstruction phase, and the checking and recovering phase. first we give the definition of reconstruction outsourcing. Reconstruction outsourcing is a method of reutilization of the cloud storage solution based on secret sharing. In this way, the reconstruction of stored data in different cloud service providers is outsourced to a cloud service provider, so that the computing resources of client hosts can be saved. In the proposed method, the reconstruction outsourcing

of pre-processed EHRs must ensure the outsourcing cloud service provider cannot obtain any content of the EHRs during the reconstruction. For accounting legitimate , we assume Health Care X is the generator of an EHR. We will show how the proposed cloud storage scheme works by taking the EHR generated by HC->X as an example. HC->X the storage and retrieval of the EHR before uploading it to the healthcare system. And the policy is used to guide the CPs for the distribution and reconstruction of the EHR. For instance, the values of n and t are decided by the policy.

1) Data Processing Phase

The Data processing operation of EHRs is executed by a healthcare system. After Health Care X uploads the EHR, denoted as a file Z and uploaded in to the Healthcare Systems(HS). The HS generate the unique ID for the EHR and computes the hash value for Z. Both ID and H(Z) are stored in the EHR systems. Then EHR systems perform Data processing by doing bitwise OR operation for Z of each block and results stored in the separate file .

Z=(X1|| ||CM){C1,… CM ∑ YP}

after performing bitwise OR operation each block results modified as
[S1 Sm]

2) Distribution Phase

The Electronic Healthcare System EHS is responsible for the distribution of Data Processed EHR. First EHS computes m polynomials . Then the healthcare system computes n shares and distributes them to CP1------CPn respectively. The shares and the identifier of the EHR are uploaded to CP by healthcare system. The identifier can be used to retrieve the processed data of EHR when a reconstruction is needed.

$$\begin{bmatrix} a_{11}, \ldots, a_{1t-1} \\ \cdots \\ a_{m1}, \ldots, a_{mt-1} \end{bmatrix} \in Z_p$$

3) Reconstruction and Outsourcing Phase

The reconstruction phase requires huge amount computational knowledge because it involves solving a large-scale system of linear equations. The client side computational workload creates extra burden for client. To make client easy handling and to improve the efficiency on the client side, we propose the reconstruction outsourcing scheme. The detailed process is discussed as follows:
Let us assume another healthcare provider HC→ Z. The healthcare system first verifies the truthfulness of HC→ X to check if it is legitimate to requested EHR. If it true, healthcare system outsources the reconstruction to a cloud service provider CPRE. Notice that here we consider the CPRE to be a curious and dishonest party, This is the strongest threat . In other words, the cloud server may return wrong computation results or steal useful information from the inputs. CPRE gets no less than t shares from CP1---------CPn to reconstruct the Processed data in EHR, cannot reveal any information useful on the original EHR. Thus, reconstruction outsourcing process is secure against the curious cloud server.

$$\begin{bmatrix} s_{11}, \ldots, s_{m1} \\ \cdots \\ s_{1k}, \ldots, s_{mk} \end{bmatrix} (k \geq t)$$

4) Checking and Recovering Phase

After getting n shares from Healthcare Systems and receiving hash of Z ,ie.,H(Z) blocks HC→ Z , recover the answers from each block of Z' and then arranging it in series. The EHR is recovered as,

Z' = b'1||…….b'm

Then HC→X, Checks the equation H(R')=H(R). If it contain the recovered Z' is true , otherwisethe recovered Z' is not real in EHR.The verification process ensures that both the cloud service providers to store the HER and the cloud service provider to execute the reconstruction outsourcing behave honest.

Table 1. Proposed Scheme Notations.

Notation	Meaning
P	Prime
t	threshold of HER
n	Number of CSP
Z	Data processing result
HC	HealthCare
EHR	Electronic Health Record

VI. PERFORMANCE EVALUATION

In our proposed scheme, we developed an application with a user-friendly interface, and conducted experiments that simulate the outsourcing process. The experiment was carried out on the Windows 10 on Intel Pentium processor of 2.70 GHz with 4 GB memory. We implemented our proposed scheme in Python, MD-5 is used as the hash function. We conducted the proof of concept experiments to show the effectiveness of the proposed scheme.In our developed application, users are allowed to define the number of servers n that the secret is distributed to, which ranges from 20-300. The threshold t is set by users as well, which ranges from 20 to 300. The experimental results are calculated as the average value of 8 executions of the algorithms.

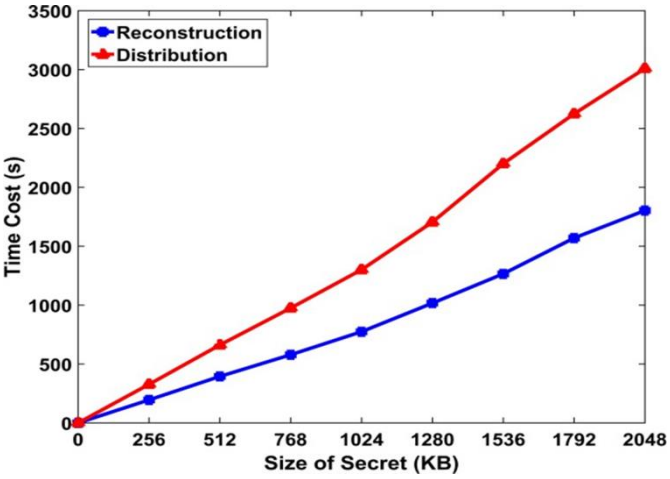

Figure 1: The time cost comparison between reconstruction and distribution phases with variational file

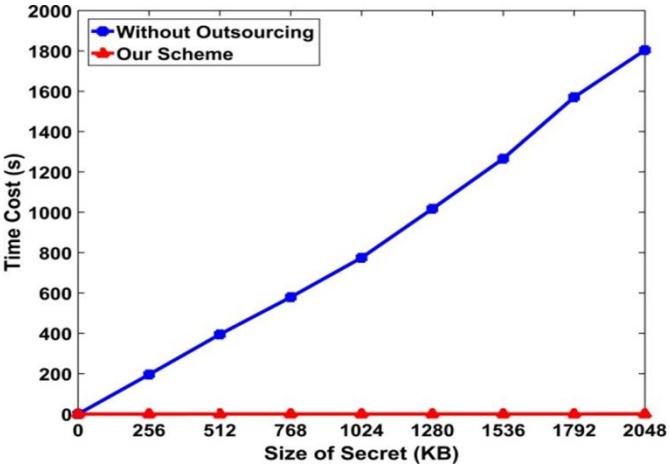

Figure 2: The time cost comparison between our scheme and reconstruction without outsourcing with variational file size

VII. CONCLUSION

In this paper, we proposed a privacy- preserving cloud-based EHR storage scheme for electronic health records based on Shamir's Secret Sharing. To highlight the problem HER to reconstruction is shared that reduce the difficulties for a healthcare center or a patient in a real-world , we proposed a secure and secret reconstruction of shared EHR for a powerful computational cloud service provider. In theoretical analysis, the previous schemes ensure the security but this scheme satisfies the security requirements. We also conducted experiments on real

documents, and the results show that, when our proposed reconstruction outsourcing approach is in place, the operation cost for healthcare centres and patients can be reduced significantly.

VIII. REFERENCES

[1]. M. J. Atallah, K. N. Pantazopoulos, J. R. Rice, and E. E. Spafford. Secure outsourcing of scientific computations. Advances in Computers, 54:215–272, 2002.

[2]. X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou. New algorithms for secure outsourcing of modular exponentiations. IEEE Transactions on Parallel & Distributed Systems, 25(9):2386–2396, 2012.

[3]. R. D'Souza, D. Jao, I. Mironov, and O. Pandey. Publicly verifiable secret sharing for cloud-based key management. In Proceedings of Indocrypt 2011, pages 290–309, 2011..

[4]. J. Gill, J. Alberto, L. Hinojosa, and I. Svecs. System: Secure cloud storage, auditing, and access control for electronic health records. 2012..

[5]. D. Hubbard, M. Sutton, et al. Top threats to cloud computing v1.0. Cloud Security Alliance, pages 1–14, 2010.

[6]. J. Lin, W. Yu, X. Yang, Q. Yang, X. Fu, and W. Zhao.A real-time en- route route guidance decision scheme for transportation-based cyberphysical systems. IEEE Transactions on Vehicular Technology, 66(3):2551–2566, 2017.

[7]. S. Salinas, C. Luo, X. Chen,W. Liao, and P. Li. Efficient secure outsourcing of large-scale sparse linear systems of equations. IEEE Transactions on Big Data, PP(99): 1–1, 2017.

[8]. A. Shamir. How to share a secret. Communications of the ACM, 22(11):612–613, 1979.

[9]. J. Yu and H. Wang. Strong key-exposure resilient auditing for secure cloud storage. IEEE Transactions on Information Forensics and Security, 2017..

[10]. H. Zhu, T. Liu, D. Zhu, and H. Li. Robust and simple n-party entangled authentication cloud storage protocol based on secret sharing scheme. Journal of Information Hiding & Multimedia Signal Processing, 4(2):110–117,2013..