International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.7 April – 2023
DOI:10.46647/ijetms.2023.v07si01.048 ISSN: 2581-4621

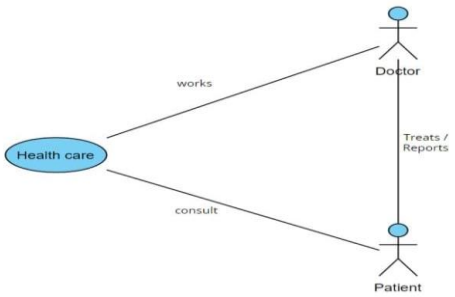
Cloud based secure and efficient framework for smart medical system using ECC

Mokkala Kiran Moni[1], B Madhusree[2], N Lavanya[3], N Manogna[4], E Pavansai Reddy[5]
[1]*Assistant Professor, Department of CSE, AITS, Tirupati*
[2,3,4,5]*Student, Department of CSE, AITS, Tirupati*

Abstract
Smart medical system (SMS) is one of the application used in architecture, which is based on communication networking along with sensor devices. In SMS, a doctor provides online treatment to patients with the help of cloud-based applications such as mobile device, wireless body area network, etc. Security and privacy are the major concern of cloud-based applications in SMS. To maintain, security and privacy, we aim to design an elliptic curve cryptography (ECC) based secure and efficient authentication framework for cloud-assisted SMS. The CSEF is secure against security attacks, and satisfies many security attributes such as man-in-the-middle attack, impersonation attack, data non-repudiation,.
Keywords: Cryptography, Cloud computing, Smart Medical System, Elliptic curve cryptography (ECC), Cloud medical system, Mutual authentication, Signature security and privacy**.**

1. Introduction

Patients receive online therapy from a doctor using cloud computing and SMS. Further details about the healthcare system's operation are available. Using an unprotected communication channel on a cloud server, the patient and doctor communicated by SMS. It causes a lot of worry that the cloud is not entirely secure. This approach raises a number of security issues, such as data confidentiality and integrity, doctor anonymity and un linkability, and patent anonymity and un linkability. Users of SMS have clear-cut privileges and direct access to the healthcare system.



The Doctor is employed by a specific hotel. In some ways, hospitality is similar to health care. Patients are advised to schedule appointments through the healthcare system. To see a certain doctor for therapy after receiving appointment authorization. People seek for doctors in the healthcare system and make appointments with them. putting together a form to take the appointment. They use a cloud database to store and retrieve data. This information can be categorised into a variety of groups that control user and system-level obligations presented a biometric and access control-based authentication framework for SMS with an adjusted structure, but which do not maintain patient unlinking capability and the medical information between patient and doctor in an open channel. Amin et al. proposed a framework for patient authentication work using wireless sensor networks in the healthcare sector. Yet, it is still necessary to provide a safe and effective authentication framework for patient, doctor, medical data, and other security features in the healthcare system, to ensure that any attacker cannot access patient or doctor data. Several plans have recently been put out to address these problems. In the suggested architecture, we develop a secure and effective mutual authentication system for SMS using ECC and the cloud. To assure security and privacy for cloud-assisted SMS, we wish to develop a secure and effective authentication system based on elliptic curve

DOI:10.46647/ijetms.2023.v07si01.048 ISSN: 2581-4621

cryptography (ECC). At CSEF, we build interactions using the ECC and the hash function. to establish communication between the Cloud and the Healthcare Center, the Cloud and the Patient, the Cloud and the Doctor, and the Cloud and the Healthcare Center. The CSEF shields users from security breaches including man-in-the-middle attacks, fraud attacks, data non-repetition, doctor anonymity, replay attacks, known-key security attributes, message authentication, patient anonymity, data privacy, and replay attacks. Session key security and session attack are just two of the many security requirements.

1.1 Related Work

- **Definition 1**. Elliptic curve discrete logarithms problem (ECDLP): For given W 1 , W 2 ∈ G to find μ ∈ Z ∗ q such that W 2 = μ W 1 , is hard .
- **Definition 2.** Elliptic curve computational DiffieHellman problem (ECCDHP): For α, β ∈ Z ∗ q and g
- **Definition 3**. The ECFP, or Elliptic Curve Factorization Problem: It is difficult to compute W 1 and W 2 in group G for,, Z q and W 1 and W 2 = W 1 + W 2. The three issues listed above are thought to be insurmountable. In other words, there isn't a polynomial-time algorithm that has a chance of solving these issues. Secondly, we discuss the rationale behind the choice of ECC for the authentication protocol used in networks for smart medical systems.

More complex :ECC is more complicated compared to RSA since it has more implementation options than a single encryption method. Therefore, the ECDLP is more challenging to solve than the discrete logarithm and factorization problems. Despite numerous authors' attempts to criticise ECC. Nonetheless, using the available computer power, it is still impossible to crack ECC. As a result, ECC's security is substantially stronger than that of other public key cryptosystems, such as RSA and Diffie-Hellman (D-H).

Smaller key size: We compare RSA ECC, which delivers equal security with smaller key sizes and lower power, bandwidth, and computational needs, as shown in Table.2. When public-key cryptography is used in low power situations, these benefits are crucial .

Computational efficiency: Since implementing scalar multiplication in software and hardware is far more practical than executing multiplications or exponentiations in them, ECC is significantly more efficient than RSA and D-H public protocols in terms of computation [

1.2 DOLEV-YAO (DY) THREAT MODEL

We take into account the Dolev-Yao (DY) model from CSEF, which has been addressed in . The following presumptions apply to any opponent A's capabilities:

A has access to the open network. A is considered to be protected, so he or she cannot get the secret key of participants. But, he or she can change, retrieve, replay, insert new message, and discard any communication network.

A is aware of the participants' collective public identification. A could be an unauthorised user or a dishonest member of the underlying communication system.

2. Algorithm

2.1 ELLIPTIC CURVE CRYPTOGRAPHY

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. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage,

2.2 DEFINITION

Neal Koblitz and Victor S. Miller separately proposed the ECC (Elliptic Curve Cryptography) technique in 1985.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.7 April – 2023
DOI:10.46647/ijetms.2023.v07si01.048 ISSN: 2581-4621

Y2 = x3 + axe + b
The main idea behind the ECC is to create a secure system for data utilising a key and an algorithm. Pic0 (E) = E where Div0 (E)

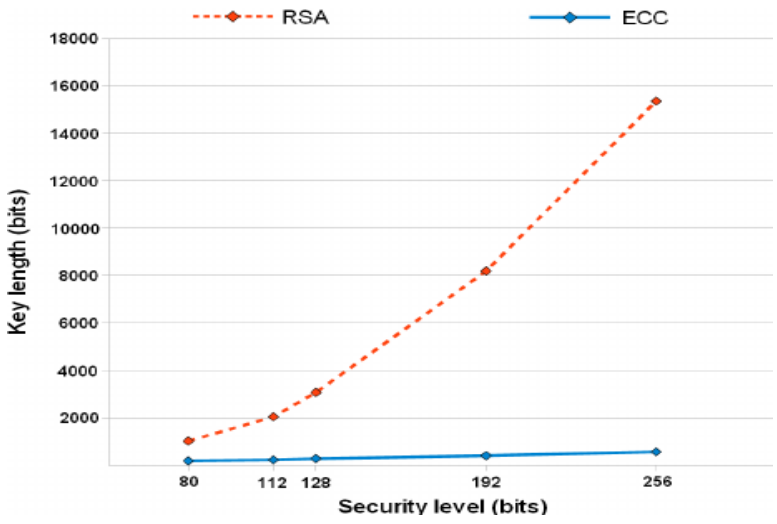
3. ANALYSIS

Both sides must agree on all of the elliptic curve's defining elements, or the scheme's domain parameters, in order to use ECC. Typically, the field size is either prime or a power of two. The length of a bit in RSA and ECC differs slightly when using the Certain formula. As a result, elliptic curve domain parameters for a range of field widths were published by various standard organisations lists several implementation factors, such as domain parameters and key sizes, projective coordinates, and fast reduction. A domain is defined by a set of parameters called the domain parameters. Due to the time-consuming and challenging computation required to determine the number of points on a curve, domain parameter construction is frequently not completed by each participant. the most significant sizes On the other side, the public key may be reduced to enable effective encryption, particularly when computing power is constrained. The contrast between the RSA method and the ECC key length . The size of the key increases when the ECC is used and decreases when the ECC is utilised. Projective coordinates, Quick Reduction, and domain parameters and key sizes are just a few of the implementation considerations mentioned in In order to add two points, one must perform many adds and multiplications as well as an inversion operation, according to the addition laws.

4. Results:

Category Type	RSA key length (bit)	ECC key Length(bit)	Key Size Ratio
A	512	112	1:5
B	1024	160	1:6
C	1536	192	1:8
D	2048	224	1:9
E	3072	256	1:12
F	7680	384	1:20
G	15360	521	1:30

Comparing the RSA and ECC key length in a bit Performance



DOI:10.46647/ijetms.2023.v07si01.048 ISSN: 2581-4621

5. Conclusion:

In order to develop a safe authentication framework in a smart medical system, security and privacy are two critical considerations. In this research, an ECC-based suitable framework for a smart medical system in a cloud environment is built. In this essay, we've covered six distinct phases, including registration, uploading patient data to the healthcare centre, treatment, check-up, and emergency phases. The security analysis of the proposed framework was demonstrated in the article. Furthermore, we've shown that the suggested framework manages security and privacy features and properties better than comparable frameworks in the same environment. We've also demonstrated that the Comparing the proposed framework to related SMS protocols, it is less expensive to compute and communicate. Hence, in a cloud-based smart medical system, CSEF is the real-world application.

6. References:

[1] S. H. Islam, M. K. Khan, X. Li, Security analysis and improvement of 'a more secure anonymous user authentication scheme for the integrated epr information system.
[2] M. Wazid, A. K. Das, S. Kumari, X. Li, F. Wu, Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for tmis, Security and Communication Networks 9 (13) (2016) 1983–2001.
[3] A. K. Sutrala, A. K. Das, V. Odelu, M. Wazid, S. Kumari, Secure anonymity-preserving password-based user authentication and session key agreement scheme for telecare medicine information systems, Computer methods and programs in biomedicine 135 (2016) 167–185.
[4] R. P. Padhy, M. R. Patra, S. C. Satapathy, Design and implementation of a cloud based rural healthcare information system model, Univers J Appl Comput Sci Technol 2 (1) (2012) 149–157.
[5] C.-L. Chen, T.-T. Yang, T.-F. Shih, A secure medical data exchange protocol based on cloud environment, Journal of medical systems 38 (9) (2014) 112.
[6] C.-L. Chen, T.-T. Yang, M.-L. Chiang, T.-F. Shih, A privacy authentication scheme based on cloud for medical environment, Journal of medical systems 38 (11) (2014) 143.
[7] R. Amin, S. H. Islam, G. Biswas, M. K. Khan, M. S. Obaidat, Design and analysis of an enhanced patient-server mutual authentication protocol for telecare medical information system, Journal of medical systems 39 (11) (2015) 137.
[8] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, S.-S. Yeo, Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks, Multimedia Systems 21 (1) (2015) 49– 60.
[9] J. Zhou, Z. Cao, X. Dong, N. Xiong, A. V. Vasilakos, 4s: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks, Information Sciences 314 (2015) 255–276.
[10] S.-Y. Chiou, Z. Ying, J. Liu, Improvement of a privacy authentication scheme based on cloud for medical environment, Journal of medical systems 40 (4) (2016) 101.
[11] P. Mohit, R. Amin, A. Karati, G. Biswas, M. K. Khan, A standard mutual authentication protocol for cloud computing based health care system, Journal of medical systems 41 (4) (2017) 50.
[12] J. Srinivas, D. Mishra, S. Mukhopadhyay, A mutual authentication framework for wireless medical sensor networks, Journal of medical systems 41 (5) (2017) 80.
[13] J. Srinivas, A. K. Das, N. Kumar, J. Rodrigues, Cloud centric authentication for wearable healthcare monitoring system, IEEE Transactions on Dependable and Secure Computing (IEEE, 2018) DOI: 10.1109/TDSC.2018.2828306.
[14] C.-T. Li, D.-H. Shih, C.-C. Wang, Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems, Computer methods and programs in biomedicine 157 (2018) 191– 203.
[15] P. Chandrakar, S. Sinha, R. Ali, Cloud-based authenticated protocol for healthcare monitoring system, Journal of Ambient Intelligence and Humanized Computing (2019) 1–17,

DOI:10.46647/ijetms.2023.v07si01.048 ISSN: 2581-4621

[16] A. Kumari, M. Y. Abbasi, V. Kumar, M. Alam, Design flaws and cryptanalysis of a standard mutual authentication protocol for cloud computingbased healthcare system, in: Advances in Data Sciences, Security and Applications, Springer, 2020, pp. 99–109
[17] P. Mohit, R. Amin, A. Karati, G. Biswas, M. K. Khan, A standard mutual authentication protocol for cloud computing based health care system, Journal of medical systems 41 (4) (2017) 50.
[18] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Rahman, M. Najmus Saqib, Security and key management in iot-based wireless sensor networks: An authentication protocol using symmetric key, International Journal of Communication Systems 32 (16) (2019) e4139.
[19] K. Mahmood, J. Arshad, S. A. Chaudhry, S. Kumari, An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure, International Journal of Communication Systems 32 (16) (2019) e4137.
[20] S. Hussain, S. A. Chaudhry, Comments on "biometrics-based privacypreserving user authentication scheme for cloud-based industrial internet of things deployment", IEEE Internet of Things Journal 6 (6) (2019) 10936–10940.
[21] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, J. J. Rodrigues, Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment, IEEE Internet of Things Journal 5 (6) (2018) 4900–4913.
[22] K. Mansoor, A. Ghani, S. A. Chaudhry, S. Shamshirband, S. A. K. Ghayyur, A. Mosavi, Securing iot-based rfid systems: A robust authentication protocol using symmetric cryptography, Sensors 19 (21) (2019) 4752.
[23] P. Gope, T. Hwang, A realistic lightweight authentication protocol preserving strong anonymity for securing rfid system, computers & security 55 (2015) 271–280.
[24] S. A. Chaudhry, T. Shon, F. Al-Turjman, M. H. Alsharif, Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber