International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.7 April – 2023
DOI:10.46647/ijetms.2023.v07si01.087 ISSN: 2581-4621

SMART MEDICAL SYSTEM USING ELGAMAL

V Sambasiva[1], N.V.R.S.Harshini[2], V.V.Supriyanka[3], S.Sai Vikas4,K.Rani[5],V.Sai Kumar[6]
Assistant professor, Student, Department of CSE, AITS, Tirupati

Abstract

Smart architecture is the concept to manage the facilities via internet utilization in a proper manner. There are various technologies used in smart architecture such as cloud computing, internet of things, green computing, automation and fog computing. Smart medical system (SMS) is one of the application used in architecture, In SMS, a doctor provides online treatment to patients with the help of cloud based applications. Security and privacy are the major concern of cloud-based applications in SMS. To maintain, security and privacy, we aim to design Elgamal Cryptography based secure and efficient authentication framework for cloud-assisted SMS.

Keywords: Cloud-based Online treatment Authentication establishment Elgamal Cryptography

Introduction

The healthcare industry is generating vast amounts of data from various sources, such as electronic medical records, medical imaging, and wearable devices. This data is critical for providing timely and accurate diagnosis, treatment, and prevention of diseases. However, the collection, storage, and processing of medical data also present
significant challenges, such as ensuring data. privacy and security, and efficiently managing large data volumes. Encryption is a public-key encryption algorithm that allows secure communication between parties without the need for a shared secret key. In the context of smart medical systems, ElGamal encryption can be used to protect sensitive medical data during transmission and while it is stored in the cloud. A cloud-based secure and efficient framework for smart medical systems using ElGamal encryption can provide a secure and efficient way to store, process, and share sensitive medical data while ensuring data privacy and confidentiality. This framework can be used to support a range of medical applications, such as telemedicine, remote patient monitoring, and medical research. The development of such a framework requires the integration of cloud computing technologies, cryptography, and medical data management.

A multidisciplinary team of experts in these domains can work together to design, implement, and maintain a cloud-based secure and efficient framework for smart medical systems using ElGamal encryption. The cloud computing is a structure of resources using different applications. To offer favourable and quick network services, a new type of cloud computing association includes a large number of processors, high-speed networks, memories and various devices are presented by users via the internet server. Cloud services offer through a web browser to get online data information. These computing strategies can be obtained by the cloud stage. that cloud services will be useful in the future. In this way, privacy and security of cloud have turned out to be important issues.

Related Work

In this section, we introduce the proposed smart contract based distributed and patient centric access control framework. In our proposed framework, we assume that each participant such as patient, hospital has registered in the national healthcare or identification system and has a unique identification number, i.e., ID. During the registration process, each entity needs to provide their personal data (Dp). Our scheme uses SHA-256 to hash the Dp and generates a unique ID based on it. Puid and Huid are the unique IDs of the patient and hospital respectively. The registration information (Dp) is stored in cloud in the encrypted form, the same way as the EMR is stored. After completing the registration process, each entity has a respective unique address in the blockchain corresponding to its unique ID. It is only accessible by the cloud server (administrator or manager) with authorized

DOI:10.46647/ijetms.2023.v07si01.087 ISSN: 2581-4621

permission from respective entity. Once registered, the cloud server will authenticate an entity's claim of credentials (unique ID, password, and private key associated with the blockchain address) and pass on the verification to the proposed system via DAuth protocol [35]. As shown in Fig. 2, our proposed framework consists primarily of four smart contracts namely Validation Contract (VC), GetAccess Contract (GAC), Grant Contract (GC), and Revoke Contract (RC), each of which implements the access control policies for a pair of entities. VC validates and verifies the registration of each participant in our proposed framework. GAC decides whether an entity gets access or not based on the agreement policies between the EMR requester and EMR owner. GC checks if there is a fair request or any misconduct by the EMR requester and grants the access permission to the requested entity for a limited span to keep the EMR secure and pseudonym. Lastly, RC revokes the access control in case of validation failure, misconduct, or bombardment of multiple requests in a short period. These smart contracts are deployed across the blockchain network to provide access to the EMR generated by IoT enabled healthcare devices. Each of these contracts are introduced in detail as follows. 1) Validation Contract (VC): During the process of validating an access request, VC verifies a specific blockchain address and ID of EMR owner and requester. It maintains an activity list to store the time whenever a new entity becomes a part of our scheme and requests access to the EMR. 2) GetAccess Contract (GAC): It includes access control agreement policies between the two entities. The main principle of GAC is to determine whether or not an individual is eligible to access a requested EMR. For that, the access control policies are verified by checking the time of the last request and the type of EMR requested. If these terms and conditions are manipulated, the RC instance will be called, and the access will be subsequently terminated. • setGuidelines(): This ABI (Application Binary Interface) is used to set access guidelines between the EMR owner and EMR requester. These guidelines are set by the EMR owner by providing various inputs such as minGap, noFR and threshold (explained in Section. • setGrant(): It takes the contract address of GC as an input to link it to GAC. GC sends misconduct reports, if any, via setGrant(). GAC then acts accordingly. • setAccessTime(): It is the ABI to set time period during which access is provided by the EMR owner. It takes values in seconds. • deleteGetAccess(): This ABI is invoked by the patient when the access control agreement and permission between the patient and other entities need to be terminated or revoked. It takes the EMR file ID, the EMR requester ID, and the access agreements as inputs to call the RC. 3) Grant Contract (GC): After satisfying all the access conditions by the GAC, GC finally provides access of an EMR to the requester for a limited period as defined in setAccessTime(). After that period is over, GC calls the instance of RC, and the access is terminated. The GC also contains the following main ABI to determine the misconduct, impose fine on the faulty requester, and update the R best solution for automated monitoring of patients in the health care industry.

Conclusion:

1. Security and privacy are two essential concerns to establish a secure authentication framework in smart medical system. we have discussed six different phases such as registration phase, health care center upload phase, patient data upload phase, treatment phase, check up phase. we have demonstrated that the proposed framework manages better security and privacy features and attributes compared to related frameworks in the similar environment. Cloud computing is required to provide a security solution to protect sensitive information and transactions. We can prevent a third party from eavesdropping or tampering with the data while it is being transmitted. Secure Healthcare Framework is designed by enhancing the Attribute Based Encryption scheme. It's a cost effective solution for storing large volumes of data. It enhances the patience experience, with the help of cloud computing, doctors and hospitals now have the power to increase patient engagement and give them anywhere anytime access to their medical data, test results and even doctor's notes. This give patients more power and control, as well as makes them more educated about their medical conditions. the

DOI:10.46647/ijetms.2023.v07si01.087 ISSN: 2581-4621

quality of health care services and reduces the human involvement in patient monitoring. Implementation of Elgamal technology in health care serves.

REFERENCES

[1] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, ‘‘Anonymous authentication for wireless body area networks with provable security,’’ IEEE Syst. J., vol. 11, no. 4, pp. 2590–2601, Dec. 2017.
[2] Y. Tsai, ‘‘Cloud computing security,’’ Commun. CCISA, vol. 18, no. 2, pp. 62–68, 2012.
[3] M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, and S. Loureiro, ‘‘A security analysis of Amazon’s elastic compute cloud service,’’ in Proc. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops (DSN), Jun. 2012, pp. 1427–1434.
[4] J. Srinivas, D. Mishra, and S. Mukhopadhyay, ‘‘A mutual authentication framework for wireless medical sensor networks,’’ J. Med. Syst., vol. 41, no. 5, p. 80, May 2017.
[5] B.-Q. Cao, B. Li, and Q.-M. Xia, ‘‘A service oriented Qos-assured and multi-agent cloud computing architecture,’’ in Proc. IEEE Int. Conf. Cloud Comput. Bengaluru, India: Springer, Dec. 2009, pp. 644–649.
[6] C.-M. Chen, K.-H. Wang, K.-H. Yeh, B. Xiang, and T.-Y. Wu, ‘‘Attacks and solutions on a three party password-based authenticated key exchange protocol for wireless communications,’’ J. Ambient Intell. Humanized Comput., vol. 10, no. 8, pp. 3133–3142, Aug. 2019.
[7] E. Casalicchio and L. Silvestri, ‘‘Mechanisms for SLA provisioning in cloud-based service providers,’’ Comput. Netw., vol. 57, no. 3, pp. 795– 810, Feb. 2013.
[8] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, ‘‘Anonymous authentication for wireless body area networks with provable security,’’ IEEE Syst. J., vol. 11, no. 4, pp. 2590–2601, Dec. 2017.
[9] Y. Tsai, ‘‘Cloud computing security,’’ Commun. CCISA, vol. 18, no. 2, pp. 62–68, 2012.
[10] M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, and S. Loureiro, ‘‘A security analysis of Amazon’s elastic compute cloud service,’’ in Proc. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops (DSN), Jun. 2012, pp. 1427–1434