International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 06 | June 2019 www.irjet.net p-ISSN: 2395-0072

IMPLEMENTATION OF CLOUDLET-BASED MEDICAL DATA SHARING USING ECC CRYPTOSYSTEM METHOD

Sonali Ekatpure[1], Prof. Subhash Pingale[2]

[1]Student, Dept. of CSE, SKN Sinhgad College of Engineering, Pandharpur, Solapur University, Solapur, India
[2]Prof. Dept. of CSE, SKN Sinhgad College of Engineering, Pandharpur, Solapur University, Solapur, India

---

Abstract - The usual framework of medical services regularly requires the sending of restitution information to the cloud, which includes sensitive customer data and causes the use of the vitality of correspondence. For all purposes, the exchange of repair information is a basic and test problem. Consequently, in this document, we develop a new structure for human services through the use of cloudlet adaptability. Cloudlet elements include security insurance, information exchange, and breakpoint location. In the information accumulation phase, we initially used the Numerical Theory Research Unit (NTRU) technique to encode client body information collected from a portable device. This information will be transmitted to adjacent cloudlets in a competent form of vitality. In addition, we show another model of trust to allow customers to choose trusted partners who need to share information stored in the cloudlet. The demonstration of trust also makes comparable patients who talk to each other about their illnesses. Third, we isolate the patient's medical information stored at a distance in three sections and provide them with adequate insurance.

***Key Words*: Privacy Protection, Data Sharing, Collaborative Intrusion Detection System (IDS), Healthcare.**

1. INTRODUCTION

Distributed computing portrays a new way, in some cases a more cost effective way, of conveying venture IT. It speaks to a genuine democratization of Web processing, as with all major problematic changes in innovation and Internet transformation, and it is not just changing the business models and the way IT foundation is being conveyed and consume, additionally the basic design of how framework create, deploy, run and deliver applications.

Healthcare covers complex processes of the diagnosis, treatment, and prevention of disease, injury, and other physical and mental impairments in humans. The patients' consumption of products and services provided by hospitals and other institutions forms the healthcare industry, which is one of the largest and fastest-growing part of a country's economy[3].

Computing resources are shared by many users. The benefits of cloud can be extended from end users to organizations. The data storage in cloud is among one of them. The virtualization of hardware and software resources in cloud eliminates the financial investment for owning the data warehouse and its maintenance. Many cloud platforms like Google Drive, cloud; SkyDrive, Amazon S3, Dropbox and Microsoft Azure provide storage services. Security and privacy are the major challenges in cloud computing. The hardware and software security mechanisms like firewalls etc. have been adapted by cloud provider. These solutions are not provides guarantee to protect data in cloud from unauthorized users. So, before storing the precious data in cloud, the data should to be encrypted. Data encryption guarantees the data confidentiality and integrity. To preserve the data secrecy we need to design a searchable algorithm that works on encrypted data.The search techniques may be single keyword search or multi keyword search. In large database the search may result in many documents to be matched with keywords. This causes difficulty for a cloud user to go through all documents and have most relevant documents. Economical searchable encryption techniques help the cloud users especially in pay-as-you use model. The researchers combined the rank of documents with multiple keyword search with efficient economically viable searchable encryption techniques[2].

In advance distributed computing, a lot of information can be put away in different clouds, consisting cloudlets and remote clouds, encouraging information sharing and intensive computations. In any case, cloud-based information sharing involves the crucial issues like, how to safeguard the security of user's body information during its conveyance to a cloudlet?, How to ensure the information appropriating in cloudlet won't cause protection issue?. As can be anticipated, with the multiplication of electronic medical records (EMR) and cloud-helped applications, an ever increasing number of considerations ought to be paid to the security issue identified with a remote cloud containing healthcare big data. How to secure the human services enormous information put away in a remote cloud?, How to successfully shield the entire framework from malicious attacks? As far as this issue, this paper proposes a cloudlet based medicinal services framework[1].

2. LITERATURE REVIEW

The functions of cloudlet consist of privacy protection, data sharing and intrusion detection. In the stage of data collection, firstly utilize Number Theory Research Unit (NTRU) method to encrypt user's body data collected by wearable devices. Those data will be send to nearby cloudlet in an energy efficient fashion. Secondly, present a new trust model to help users to select trustable partners who want to share stored data in the cloudlet. The trust model also helps identical patients to communicate with each other about their diseases. Thirdly, divide users medical data stored in remote cloud of hospital into three parts, and give them proper protection. Finally, in order to protect the healthcare system from malicious attacks, design a novel collaborative intrusion detection system (IDS) method depend on cloudlet mesh, which can effectively prevent the remote healthcare big data cloud from attacks[1].

We have to define and solve the challenging issue of privacy preserving multi-keyword ranked search over encrypted cloud data (MRSE). They establish a set of strict privacy requirements for such a secure cloud data utilization system. Among various multikeyword semantics, they choose the efficient similarity measure of "coordinate matching", i.e., as many matches as possible, to capture the relevance of data documents to the search query. They further use "inner product similarity" to quantitatively evaluate such similarity measure. First propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. Thorough study of inspecting privacy and efficiency guarantees of proposed schemes is given[2].
A practical solution for privacy preserving medical record sharing for cloud computing developed on the basis of the classification of the attributes of medical records, they use vertical partition of medical dataset to achieve the consideration of distinct parts of medical information with different privacy concerns. It mainly consisting four components, i.e., (1) vertical data partition for medical information publishing, (2) data combining for medical dataset accessing, (3) integrity checking, and (4) hybrid search across plaintext and ciphertext, where the statistical analysis and cryptography are innovatively combined together to provide multiple paradigms of balance among medical data utilization and privacy protection. A prototype system for the huge scale medical data access and distributing is implemented[3].

3. PROPOSED WORK

The implementation for a given input of different medical dataset, apply efficient medical data sharing with KDC method for secure data sharing in cloudlet. Figure demonstrates how the proposed system works. The description of the system is as follows:

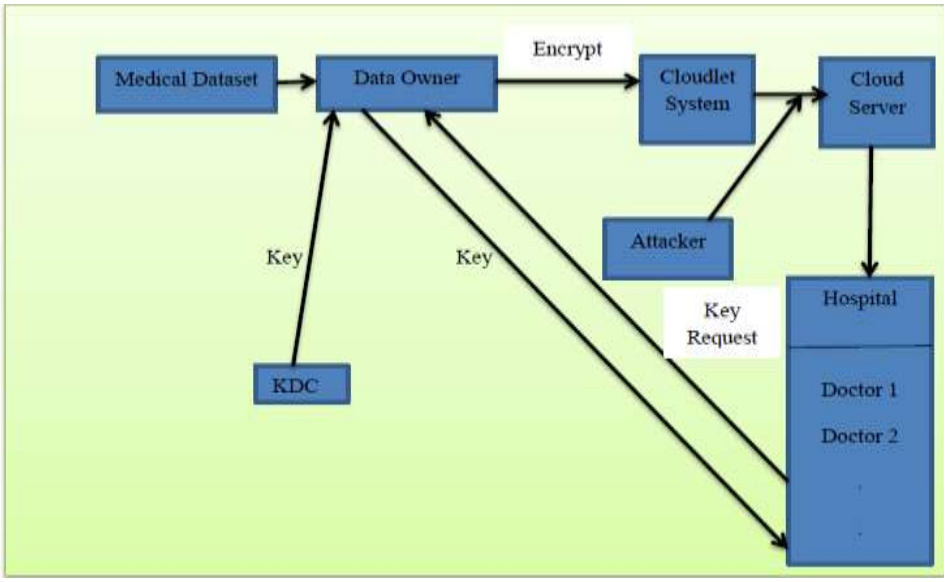

Fig-1-Block diagram of system

In this system data owner take medical dataset as an input to the system. Then data owner encrypt the data using ECC key encryption algorithm. This used to protect the user's medical data from being leaked or abused. This scheme is to protect the user's privacy when transmitting the data to the cloudlet. The key distribution center (KDC) provides the key to data owner for encryption. The data owner store encrypted data in a cloudlet system. The cloudlet system likely for them to share common

aspects, for example, patients suffer from similar kind of disease exchange information of treatment and share related data. For this purpose, system use users' similarity and reputation as input data. This encrypted data stored in a cloud server. While storing data in a cloud server the attacker may attack on it and try to leak the data. In order to protect the healthcare system from malicious attacks, we develop a novel collaborative intrusion detection system (IDS) method based on cloudlet mesh, which can effectively prevent the remote healthcare big data cloud from attacks. If in any hospital doctors need to use user's data from cloud, then doctor send key request to the data owner. If authenticated doctor is found then data owner provide a key to decrypt the data. Using this key doctor access the data from cloud server, decrypt and read it.

3.1 Module Descriptions

1. Input Dataset

This system used medical dataset as an input for securely sharing in cloudlet-based system.

2.Data Owner

The work of data owner is taking a medical dataset, encrypt it using ECC encryption algorithm and store it cloudlet. For encrypt the data, data owner get key from KDC and for decryption data owner provide the key to authenticated user/doctor.

3. Key Distribution Center (KDC)

The key distribution center is used to reduce the risk of key exchanging. It distributed the key among data owner and authenticated user. Using this approach proposed system save both time and memory.

4. Cloudlet System

The Cloudlet system store the encrypted data provided by the data owner and also share it to the cloud server. While sharing if any attack found then it prevent it using collaborative intrusion detection system (IDS) method.

5. Cloud Server

The cloud server is used to store the user's encrypted data. If any authenticated doctor wants to access the data then it can be access from the cloud. For decrypt the data he/she must send a key request to the data owner

4. CONCLUSION

This system proposed a protected cloudlet-based information sharing framework. This framework share information in encoded design. For encryption, KDC give the way to the customers/information proprietor and they encode the information utilizing encryption calculation. While sharing information, if attack is happened then it prevents by the cloudlet utilizing collaborative intrusion detection system (IDS) technique. The execution of framework is demonstrates that this framework is more secure and trustable. It likewise spares the time and memory.

REFERENCES

[1]. Min Chen, Yongfeng Qian, Jing Chen, Kai Hwang, Shiwen Mao, Long Hu, "Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing", IEEE Transactions on Cloud Computing, 2016.
[2]. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.
[3]. J.-J. Yang, J.-Q. Li, and Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," Future Generation Computer Systems, vol. 43, pp. 74–86, 2015.
[4]. K. Hung, Y. Zhang, and B. Tai, "Wearable medical devices for telehome healthcare," in Engineering in Medicine and Biology Society, 2004.IEMBS'04. 26th Annual International Conference of the IEEE, vol. 2. IEEE, 2004, pp. 5384–5387.
[5]. M. S. Hossain, "Cloud-supported cyber–physical localization framework for patients monitoring," 2015.
[6]. J. Zhao, L. Wang, J. Tao, J. Chen, W. Sun, R. Ranjan, J. Kołodziej,A. Streit, and D. Georgakopoulos, "A security framework in g-hadoopfor big data computing across distributed cloud data centres," Journal of Computer and System Sciences, vol. 80, no. 5, pp. 994–1007, 2014.M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring," Computer Networks, vol. 101, pp. 192–202, 2016.
[7]. R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on. IEEE, 2010, pp. 268–275.
[8]. K. He, J. Chen, R. Du, Q. Wu, G. Xue, and X. Zhang, "Deypos:Deduplicatable dynamic proof of storage for multi-user environments,"2016.
[9]. N. Cao,"Privacy-preserving multi-keyword ranked search over encrypted cloud data",INFOCOM, 2011 Proceedings IEEE,IEEE, (2011).

[10]. M. Quwaider and Y. Jararweh, "Cloudlet-based efficient data collection in wireless body area networks," Simulation Modelling Practice andTheory, vol. 50, pp. 57–71, 2015./

BIOGRAPHIES

Ms. Sonali A. Ekatpure is currently pursuing M.E(Computer)from Dept of Computer Science &Engineering, SKN Sinhgad College Of Engineering, Korti, Pandharpur Maharashtra, India -413304.She received her B.E(Computer) Degree from Shivnagar Vidya Prasarak Mandal's College of Engineering, Malegaon(Bk),Maharashtra, India -413115. Her area of interest is Cloud Computing Network Security.

Prof. Subhash V. Pingale is currently working as Asst. Professor with Dept of Computer Science &Engineering, SKN Sinhgad College Of Engineering, Korti, Pandharpur Maharashtra, India -413304. His research interests include Image Processing and Networking.