ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

Efficient and Secured-Privacy Medical Data Sharing in IOT using Online/Offline Technology

Dr. P. KALYANI
[1]Professor, Department of MCA,Narayana Engineering College, Gudur, Nellore

M. Srivalli.
[2]PG Scholar, Dept. of Master of Computer Applications, Narayana Engineering College, Gudur. Nellore

ABSTRACT

Implementing the Internet of Things(IOT) in Medical Departments, Healthcare providers can track patients adherence to treatment plans and thereby provide immediate help and service whenever the people needed according to their conditions. IOT allows Medical Professionals to be more connected with the patients. So for providing the security to the patients data, the collected big data from the smart Medical terminal devices is encrypted and stored in a cloud server, so only authorised users are allowed to access. As the smart terminals have usually limited computing power, it leads to users Privacy issues. To solve this privacy issues in sharing users data we introduced an efficient and secured-privacy data sharing scheme in this journal. To handle this challenging issue, we will eliminate the attribute matching function and use attribute bloom filter to conceal all the attributes in the access control structure. To make it even more efficient and User-friendly, we introduce the Online/Offline technology in the encryption phase. Before the message is entered, a huge amount of work which is needed at the encryption stage is done readily. Then once the text is entered, it generates the ciphertext quickly. Besides, the initialization stage of the system does not to enter all the attributes. If the overall attributes of the system users increase, there is no need to reinitialize the system, which is an addition to system efficiency. The Security analysis and the performance analysis proves that the sharing scheme is providing a secured-privacy to the users data and the data processing in IOT based data sharing**.**

KeyWords:

Attribute-based Encryption, Attribute Bloom Filter, Data sharing, Secured-Privacy preserving.

INTRODUCTION

The implemention of Internet of Things(IOT) along with the application of information andcommunication technology is affectiong our daily life in an efficient way. The Internet of Things is generally made up of many diverse intelligent objects

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

like our smartphones, smart watches etc., that can collect lots of information of users. Because of its distributed characteristics of IOT, to share the collected information with the other people and smart devices, it requires a flexible access control strategy. How to control data access and provide more flexibility is now an urgent problem. To solve this problem, we will introduce a technology called Attribute-Based Encryption(ABE).

In this attribute-based encryption system, the particular ciphertext is decrypted by a specific private key only when the access control policy matches with the users attribute set. To provide the more flexibile access policies, the attribute enryption is divided into CP-ABE and KP-ABE, based on whether ciphertext is contacted with the attributes of the users or access control policy. The CP-ABE is more suitable to control the data access. In the CP-ABE system, the ciphertext is linked to an access control structure in the encryption stage while the users private key is linked with the attribute sets while generating a secret key. The control access strategy can be managed flexibly by the data owner. For the visitors, the decryption of ciphertext is only possible when the attribute set of users matches the predefined access structure.

The IOT based systems are now making a communication revolution. IOT provides a better means of communication between the patients and doctors using smart health systems. If the doctor is alerted intime about the critical conditions of a patients he will be saved. The medical sensors are used to collect various sensitive data related to health of the user. Then these medical records are sent through IOT and stores those records on cloud server. Users can share their medical inormation through IOT with the help of medical terminals. While sharing the data, privacy and security of data is the main concern when the data is exposed to an open network. One more problem is, the sensors and smart terminals are resource constrained device and the quick generation of the ciphertext which is stored in cloud is another problem.

BACKGROUND WORK:

To overcome the above mentioned hurdles and problems we need to make the following implementations:

Primarily, when ciphertext is entered in cloud server, the control structure is also uploaded. By removing the attribute matching function, we can hide the attributes into access structure. The access control structure also causes leakage of user privacy. To hide the entire attributes in an anonymous access control structure we have to use the Attribute Bloom Filter(ABF). So, the data stored in cloud is server is secure now.

Secondly, the immediate response to the user activity is needed. For this we have to generate the ciphertext qiuckly. So we use Online/Offline encryption technology. In this technology lots of preliminary works of encryption are done readily before the information is known. When the information is entered, it quickly generates the ciphertext to it. Thereby this Online/Offline encryption technology ensures the efficiency of the encryption.

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

Finally, to add more efficiency, the initialization phase of the system does not requied to mention all the attributes. Whenever the users increase, there is no need for system reinitialization. This makes our scheme more efficient.

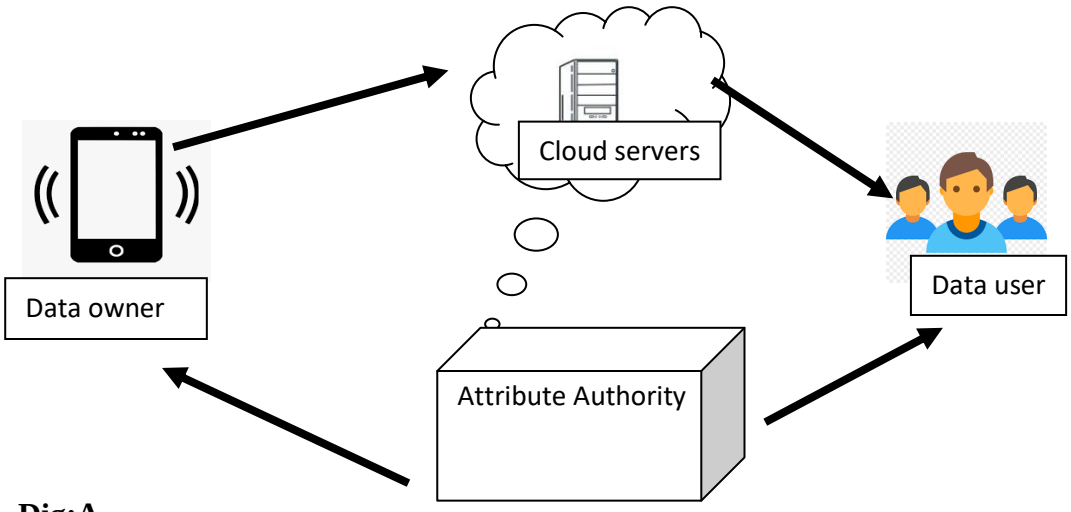
BLOOM FILTER:

Bloom Filter is introduced in the year 1970. This is very effective in probabilistic data structure on the storage space. This technology is used to check whether an element is exists in a specified set very quickly and efficiently.

It helps to know whether element either definitely is not the set or may be a part in the set.

SCHEME MODEL:

The medical data sharing scheme is having four entites and they are as



Dig:A

Cloud Server:

The cloud server is used to store the users sensitive information and also stores the access control structure which is specified by the constraints of the data owner. It also stores the Attribute Bloom Filter and cipher text. It is the virtual data storage system.

Attribute Authority:

The Attribute authority controls and manages all the attributes of the system. It generates the attribute public key to the system and it generates the attribute private key to the users of data. This attribute authority is completely reliable.

Data User:

Generally in our system the users of the data are the doctors and family or friends of the data owner. People who want to access the data should provide the

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

parameters matching the attributes constrains. Then if constraints matched he will get the access to the data by generating ciphertext.

Data Owner:

Here owner of the data in our system is patient who wants to share data with doctors and family. The information is collected from the smart medical devices like smart watches through the sensors. Then ciphertext is generated and the bloom filter and access control structure are uploaded to the cloud server. This is controlled by the data owner.

PROPOSED WORK:

The algorithm section of the medical data sharing scheme is consists of the following :

Initialisation:

L→(PK,MSK)

It is executed by the attribute authority. It considers the L as input and then generates the public key PK and the master secret key MSK as output.

Key Generation:

(PK,S,MSK)→SK

This algorithm is executed by the attribute authority. It accepts the public parameters PK, the master secret key MSK, and the attribute set of the users S as inputs. It generates the secret key SK as output.

Encryption:

(PK,m,(M,p))→(CT,ABF)

Encryption phase consists of three sub phases. They are Online Encryption, Offline Encryption, ABFbuild.

Offline Encryption:

(PK)→IT

The data owner gives public parameters PK as inputs and gets cipher text IT as output.

Online Encryption:

(PK,IT,m)→CT

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

The public parameter PK is taken as input by the sensors and smartphones, cipher text IT and message m to be encrypted and also the access control structure. Then cipher text CT is the output.

ABFbuild:

(M,P)→ABF

The input here is control access structure (M,p) taken by the data owner and generates the output attribute bloom filter.

Decryption:

(M,ABF,PK,SK,CT)→m.

It is executed by the data user, it contains two sub algorithms and they are as follows:

ABFQuery:

(S,ABF,PK)→p

The attribute set s, ABF and private key PK are considered as input and ABF Query algorithm generates the reconstructed attribute mapping p=(rownum,attr). The mapping shows the row number of matrix M and all the attributes s.

Decrypt:

(SK,CT,(M,p))→m or !

The secret key SK, the ciphertext CT and reconstructed attribute mapping pare the inputs of the data user. It returns message m only when attributes are satisfies the access constraints. Otherwise it outputs !.

PROPOSED SCHEME:

It consists the following steps:

SYSTEM INITIALISATION:

The attribute authority takes a security parameter λ , and selects a group G of primer p , g as a generator . It expresses the maximum bit length of attributes in the system. Lrn expresses the maximum bit length of the row numbers of access matrix. $LABF$ expresses the size of bit array of the ABF . k expresses the number of hash functions associated with the ABF . Then, it randomly choose $\alpha,a,\in Y*p$ and it generates k hash functions H1(),H2(),…,Hk() which maps an element to a position in the range of [2,LABF] .

The public key and the master secret key are as follows

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

PK=MSK=<G,g,ga,e(g,g)α,Lat,Lrn,LABF,H1(),H2(),…,Hk(),l,H>.(α).

MSK= α.

KEY GENERATION:

Every data owner and data user must register and authenticate to the attribute authority to generate the key. If they are not liable, it will be stopped. Otherwise they will assign attributes and the secret key related to the attributes set s.

The attribute authority chooses a number randomly **t,x1,x2,…,x|S|** and calculates **hi=gxi** and **K=gαgat, K0=gt, Ki=hti for i∈S .** Then, it takes inputs as the *PK* , the *MSK* and an attribute set *S* , and it gives the outputs as private key related to attribute set *S* :

SK=(S,K,K0,{Ki}i∈S).

DATA ENCRYPTION:

The sensors and smart phones stores the lot of prerequisite work of encryption which helps in quick generation of ciphertext. The intermediate ciphertext and the attribute bloom filter are the examples. So the ciphertext is quickly generated when we user wants a response immediately.

Offline Encryption(PK):

The public parameter PK, is the input only given by data owner. The maximum bound of matrix M is P.

key=e(g,g)αs,C3=gs.

→Forj=1 to p, randomly picks and computes:

C2,i=gaλ′ih−rii,C3,i=gri.

→The intermediate ciphertext is

IT:=(s,λ′i,key,C3,{C2,i,C3,i}i∈[1,p]).

- **Online Encryption** :

The data owner selects randomly **y3,y4,…,yk∈Zx** , sets the vector **y=(s,y3,y4,…,yk)T** and computers a vector of shares of **s** as **(λ1,…,λl)T=My** . The public parameters **PK** , an intermediate **IT** , and an LSSS access structure **M** , where **M** is an **l×n** matrix, and where **l≤p** will be stored on the sensors and the smartphones.

The ciphertext will be generated quickly by the system using the medical terminals.

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

For i=1 tok.

C2=C4, ;where i=key·m

λi−λj.

The final CT cipher text is,

CT:=((M,ρ), C1, C2, {C2,i,C3,i,C4,i}i∈[1,p]).

ABFbuild:

The access policy (M,p) is entered as input by the data owner. we need to lower the false positve property in the BloomFilter. This is to locate the attributes to corresponding row number very precisely. Let the length of the number of a row is i , set of elements is Se.

When an element **e** in the set **Se** will be added to the ABF, this algorithm first randomly generates k-1and bit strings **r2,e,r3,e,…,rj−1,e** , then sets

rk,e=r1,e*r2,e…*e.

Thus the algorithm shares the element e with secret sharing scheme.

Then it calculates values of the hash function ofattribute atte and having k independent unique disgtributed hash functions **H0(),…,Hi().**

H0(atte),H1(atte),…,Hi(atte).

Finally the ABF will be storedin the smart devices and the sensors. And will upload the data to the cloud servers.

DATA DECRYPTION:

The data will be decrypted only when the user of the data is satisfies the attribute constraints which are set by the data owner.so that only the authorised users and authenticated users will be able to access control structure.

ABF Query:

User will provide the set of attribute set s, the ABF and parmeter key as the input to the ABFQuery system.

→the algorithm computes the y hash functions **H2(),…,Hi()** and obtains

H2(att),H3(att),…,Hi(att).

Then, the algorithm gets the corresponding strings from the positions as follows:

Hj(att) position in ABF →r. i,e for j∈{1,…,k}.

Decryption:

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

Dec(SK,CT,(M,p))→m or l.

The data user gives SK as input, the CT as ciphertext. And the matrix of access (M,p). If it satisfies N, it gives output ! otherwise it calculates the algorithm as follows:

key=e(C2,K);

for j∈j(e(K0,C1,j·ga·C3,j)e(Kj,C2,j))j=e(g,g).

Next, the returns the message is

N=C1e(g,g).

CONCLUSION:

In this journal, the secured medical data sharing in the Internet Of Things using our scheme in the cloud storage is presented. In our security scheme, we had suggested to remove the Attribute Based Encryption and to make the efficient scheme is suggested which is called as the ABF(Attribute BloomFilter). This ABF is used to filter the unauthorised access and help in spam filtering of the data entered in the access control structure. The efficiency of the scheme is boosted by the implementation of the Online/Offline encryption technology. In this technology the pre-requisite work which is needed to be done in the encryption phase is made done readily. So thereby when the data is received as the input by the data owner or user the cipher text is generated. This is an addition to the efficiency of the proposed scheme. The ciphertext is generated only when the user who is trying to access the data stored in the cloud should provide the data that matches the constraints of the attributes. We don't need to reinitialise the system whenever the number of users constraints and attributes are increased. Finally the secured-privacy ensured medical data sharing scheme through the medical data sharing in the cloud storge using Internet Of Things is proposed efficiently.

References:

1. D. Zheng, A. Wu, Y. Zhang, and Q. Zhao, "Efficient and privacy-preserving medical data sharing in Internet of Things with limited computing power". IEEE Access, vol. 6, 28019-28027, 2018.

2. R. Boussada, B. Hamdane, M. E. Elhdhili, and L. A. Saidane, "Privacy-preserving aware data transmission for IoT-based e-health". Computer Networks, vol. 162, 106866, 2019.

3. K. Gai, K.K..R Choo, M. Qiu, and L. Zhu, "Privacy-preserving content-oriented wireless communication in internet-of-things". IEEE Internet of Things Journal, vol. 5, no. 4, pp. 3059-3067, 2018.

4. S. Hohenberger, and B. Waters, "Online/offline attribute-based encryption. In International workshop on public key cryptography", Springer, Berlin, Heidelberg, pp. 293-310, 2014.

5. H. Ma, Z. Wang, and Z. Guan, "Efficient ciphertext-policy attribute-based online/offline encryption with user revocation". Security and Communication Networks, 2019.
6. J. Jeong, J. W. J Joo, Y. Lee, and Y. Son, "Secure cloud storage service using Bloom filters for the internet of things", IEEE Access, vol. 7, 60897-60907, 2019.
7. S. Jegadeeswari, P. Dinadayalan, and D. Gnanambigai, "Efficient Dynamic Bloom Filter Hashing Fragmentation for Cloud Data Storage", Cybernetics and Information Technologies, vol. 19, no. 1, pp. 53-72, 2019.
8. R. Jain, M. Rawat, and S. Jain, "Data optimization techniques using Bloom filter in Big Data", International Journal of Computer Applications, vol. 142, no. 3, pp. 23-27, 2018.
9. J. Bruck, J. Gao, and A. Jiang, "Weighted bloom filter. In 2006 IEEE International Symposium on Information Theory", IEEE, pp. 2304-2308, 2006.
10. V.S. Viswanth, R. Ramanujam, and G. Rajyalakshmi, "A review of research scope on sustainable and eco-friendly electrical discharge machining (E-EDM)". Materials Today: Proceedings, vol. 5, no. 5, pp. 12525-12533, 2018.

11. I. H. Arka, and K. Chellappan, "Collaborative compressed I-cloud medical image storage with decompress viewer", Procedia Computer Science, vol. 42, pp. 114-121, 2014.
12. G. Zhiqiang, H. Lingsong, T. Hang, T and L. Cong, "A cloud computing based mobile healthcare service system" In 2015 IEEE 3rd International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA), IEEE, pp. 1-6. 2015.
13. W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang and G. Wang, "Security and privacy in the medical internet of things: a review", Security and Communication Networks, 2018.
14. K. A. N. Kai, Z. B. Pang, and W. A. Cong, "Security and privacy mechanism for health internet of things" The Journal of China Universities of Posts and Telecommunications, vol. 20, pp. 64-68, 2018.
15. V.S. Viswanth, R. Ramanujam, and G. Rajyalakshmi, "A Novel MCDM Approach for Process Parameters Optimization in Eco-Friendly EDM of AISI 2507 Super Duplex Stainless Steel". Journal of Advanced Research in Dynamical and Control Systems - JARDCS, vol. 10, no. 7, pp. 54-64, 2018.
16. J. Ling, and A. X. Weng, "A scheme of hidden-structure attribute-based encryption with multiple authorities", In IOP Conference Series: Materials Science and Engineering, IOP Publishing, Vol. 359, No. 1, p. 012-015, 2017.
17. Rajasekar, P. and Mangalam, D. (2016) Efficient FPGA implementation of AES 128 bit for IEEE 802.16e mobile WiMax standards. Circuits and Systems, 7, 371-380. doi: 10.4236/cs.2016.74032.

18. C. Wang, and J. Luo, "An efficient key-policy attribute-based encryption scheme with constant ciphertext length", Mathematical Problems in Engineering, 2013.

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

Dr.P.Kalyani ,Professor, Department of MCA,Narayana Engineering College Gudur.She received her MCA from Sri Venkateswara University-Tirupati in 2006.Ph.D from Sri Venkateswara University – Tirupati in 2018.Her areas of Research :Spatial Data mining,Remote sensing,GIS,IOT.

M. Srivalli has received her B.Sc degree in Vidyalaya Degree College, Gudur, affliated to VSU in 2017. And pursuing MCA at Narayana Engineering College(NECG) Gudur, AP affliated to JNTU, Ananthapuramu in (2017-2020).

