Enhanced Data process, storage, and retrieval in e-healthcare system

Mr. K. Jaya Krishna 1, Mr. Madira venkata Ranga Reddy 2
#Associate professor in the department of CSE at QISCET(Autonomous), Vengamukkapalem,Prakasam (DT)
#MCA Student in the department of MCA at Qis College of Engineering and Technology(autonomous), Vengamukkapalem, Prakasam (DT)

ABSTRACT_

A growing number of people in the e-healthcare system receive top-notch medical care by sharing their encrypted personal health records (phrs) with physicians or organisations engaged in medical research. One significant problem, though, is that the encrypted files make it difficult to search for information effectively, which reduces the amount of data used. Another problem is that the process of providing medical care necessitates a doctor's constant availability online, which may be too expensive for certain professionals to afford (for example, to be absent occasionally). Here, we develop a new, practical, and secure proxy searchable re-encryption method that enables medical service providers to conduct remote phrs monitoring and research in a secure and effective manner. Through our DSAS scheme, (1) patients' healthcare records collected by the devices are encrypted before uploading to the cloud server ensuring privacy and confidentiality of phrs,

(2) only authorised doctors or research institutions have access to the phrs, (3) Alice (doctor- in-charge) is able to delegate medical research and utilisation to Bob (doctor-in-agent) or certain research institution through the cloud server, supporting minimising information exposure to the public, and (4) Alice can access Bob's (do We formalise the definition of security and demonstrate our scheme's security. Finally, performance analysis demonstrates the effectiveness of our plan.

1.INTRODUCTION

The e-healthcare sensor network is now ready for commercial adoption and deployment thanks to the rapid development of artificial intelligence and wearable devices and sensors. E-Medical services sensor network filling in as a portable stage significantly benefit patients to get clinical therapy of top notch and proficiency. Patients' devices, as depicted in Fig. 1, collect a significant amount of personal healthcare records through sensor devices. By utilizing this data, doctors are able to more effectively

diagnose and address the needs of patients. Such data likewise empowers clinical scientists and experts to perform investigation to acquire better experiences on sicknesses and devise better therapies. In any case, these information might be put away on distributed storage given by outsider specialist co-ops [10], [16], [34], which present potential security issues like information spillage. This is because once the data is outsourced, neither the patients nor the doctors have control over the information. As a result, the confidentiality and privacy of these outsourced data ought to be safeguarded in such an environment. For instance, some healthcare facilities authorize the use of large amounts of patient health records (PHRs) by the Centers for Disease Control and Prevention (CDC) on cloud servers. Doctors at the CDC are allowed to use data mining technology to study these data in order to make disease prevention and control easier. Be that as it may, during the time spent gathering case data from clinical establishments and the execution of conventional information mining innovation, the CDC may unavoidably uncover delicate information of patients. It is extremely difficult to store, manage, and retrieve the phrs in a secure and effective manner.E-medical care framework requires more grounded security and protection ensures for rehearses concerning the two information and admittance to information. All phrs stored in the cloud should be encrypted to prevent information leakage [11], [14], [15], [26], [27], and [42]_[44]. Encryption can be used to address concerns about data privacy, prevent attacks from malicious users and cloud servers, and ensure data confidentiality, but it also introduces user inconvenience. For example, ordinary encryption strategies render it dif_-religion to question these scrambled information [28] on account of the futile data recovery techniques in view of plaintext. Because of this impediment of customary, the majority of the investigates utilizes accessible encryption (SE) cryptosystem to ease such worries. With accessible encryption innovation, patients in the e-medical care framework initially scramble the likely watchword as a record and afterward transfer it to the cloud server alongside the encoded phrs. Then, the approved specialist or examination establishment can work encoded catchphrase search by sending a secret entryway produced with a specific watchword to the cloud server. With the hidden entrance, the cloud server can work watchword search over the scrambled list and recover the comparing records. Generally, an accessible encryption cryptosystem permits the cloud server to look through encoded information for

clients without finding out about catchphrases or plaintext.Doctors at the CDC can use searchable encryption technology to retrieve information from encrypted patient records and administer medical care. In any case, such a framework likewise suggests the specialists should be accessible constantly. Treatment would be impossible if the doctor were not available. Intermediary re-encryption (PRE) [4], [5], [36] was proposed to take care of the above issue by permitting a confided in intermediary to safely change figure message having a place with one specialist to another so a specialist can designate the clinical treatment right to the next specialist in his missing. Take, for instance, the two physicians Alice and Bob. Every patient with Alice's public key can encode the medical care records to Alice. Let's say Alice wants to delegate the decryption authority to Bob while she is away on vacation. The re-encryption key enables the proxy to re-encrypt a cipher text encrypted under Alice's public key into a cipher text of the same message encrypted under Bob's public key using PRE technology, which allows Alice to generate an encryption key based on his private key and Bob's public key. The current PRE method, on the other hand, has two drawbacks. To begin with, the intermediary is excessively strong: The proxy can transform all Alice cipher texts using the re-encryption key, regardless of the cipher text's keyword. Second, inborn from the bidirectional property, it is difficult to give intrigue opposition when the deceptive intermediary plots with the representative to trade the delegator's confidential key, which comprises a serious security issue to the framework since now the agent can mimic as the delegator. As a result, it is necessary to limit the proxy server's capabilities.

2.LITERATURE SURVEY

2.1 Enabling privacy-preserving multi-server collaborative search in smart healthcare

Abstract

With the advancement of smart healthcare, each medical institution stores huge amounts of users’ medical data in its cloud server for diagnosis and treatment. However, the traditional storage structure has obstacles to reasonable medical resources access and medical data circulation, such as data security, query privacy, and isolated data island problems. An intuitive solution is to store all the encrypted medical data in a central server. But this method absolutely depends on the central server, causing more performance disadvantages and privacy risks. Therefore, it is urgent to construct a secure

and proper medical data retrieval scheme. Based on the existing data storage model, we build a multi-server search scheme to collaboratively perform diagnostic institution location, medical data search, and even cross-domain data search in this paper. The multi-server architecture solves problems of destructiveness and information over-centralization caused by the single server and enhances the reliability and practicality of the system. The utilization of hidden vector encryption, secret sharing, and secure multi-party computation realizes efficient search, identity privacy, search pattern security, and access pattern security. Security analysis demonstrates that identity privacy and query security are protected. Extensive experiments show that the scheme has better data search and data add efficiency through horizontal and vertical comparisons.

2.2 Secure data sharing in cloud and iot b e data sharing in cloud and iot by leveraging attribute-based aging attribute-based encryption and blockchain

MD Azharul Islam

ABSTRACT

Data sharing is very important to enable different types of cloud and iot-based services. For example, organizations migrate their data to the cloud and share it with employees and customers in order to enjoy better fault-tolerance, high-availability, and scalability offered by the cloud. Wearable devices such as smart watch share user's activity, location, and health data (e.g., heart rate, ECG) with the service provider for smart analytic. However, data can be sensitive, and the cloud and iot service providers cannot be fully trusted with maintaining the security, privacy, and confidentiality of the data. Hence, new schemes and protocols are required to enable secure data sharing in the cloud and iot. This work outlines our research contribution towards secure data sharing in the cloud and iot. For secure data sharing in the cloud, this work proposes several novel attribute-based encryption schemes. The core contributions to this end are efficient revocation, prevention of collusion attacks, and multi-group support. On the other hand, for secure data sharing in iot, a permissioned blockchain-based access control system has been proposed. The system can be used to enforce fine-grained access control on iot data where the access control decision is made by the blockchain-based on the consensus of the participating nodes.

3.PROPOSED SYSTEM

Uni-Directional: Uni-directional intermediary re-encryption is more prevalent than multi-directional intermediary re encryption, in any case, the delegatee may pass consents to an outsider, which will build the divulgence of security. Consequently, unidirectionality is a vital trademark for e-medical care framework.

Intermediary Undetectable: In the protected e-medical services framework, on the off chance that a vindictive client can recognize a re-scrambled ciphertext from a unique ciphertext, it will build the security hazard, for example, the malevolent client knows the delegator is

Not accessible at the present time. Subsequently, e-medical care framework should give intermediary undetectable.

Condition-Stowing away: In the contingent intermediary re-encryption plot, the condition frequently contains some confidential data. In the event that the condition is uncovered, it will make an extraordinary misfortune the framework. Clearly, assuming that the intermediary condition is covered up, the intermediary server will get less delicate data, which makes the e-medical care framework safer.

Arrangement Opposition: Intrinsic from reliable prop-erty, it is difficult to give intrigue obstruction when the unscrupulous intermediary conspires with the delegatee

To trade the delegator's confidential key, which would be a debacle to the e-heathcare framework. As these approved work are normally worked on the intermediary server (thought to be an outsider specialist organization), which for security reason is thought to be untrusted. Consequently, giving conspiracy opposition in a solid e-medical care system is fundamental

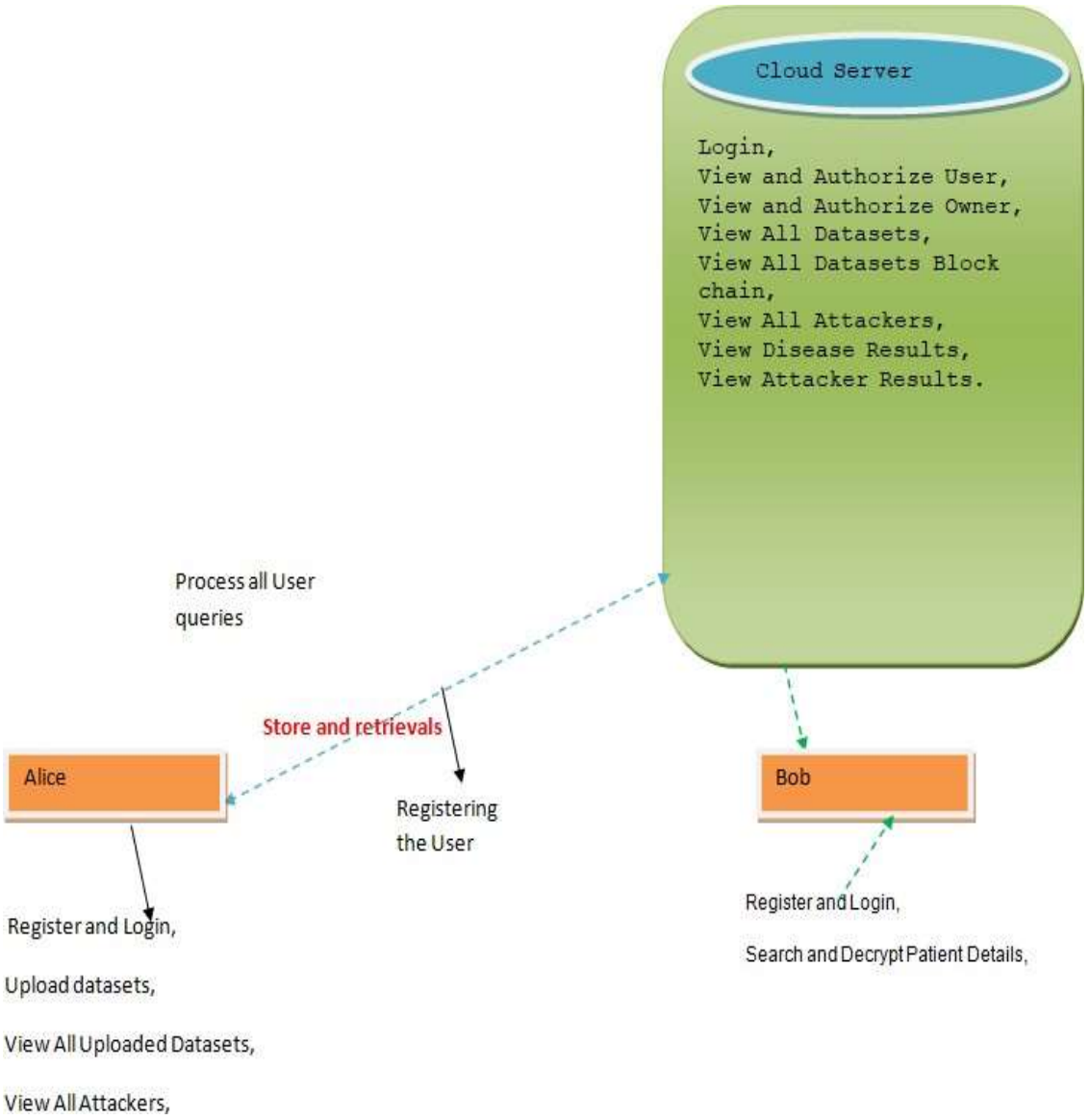

Fig 1:Architecture

4.RESULTS AND DISCUSSION

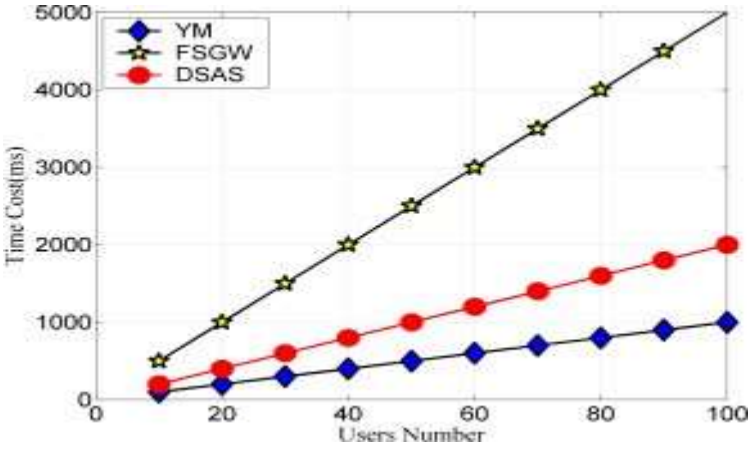

FIGURE 2. Performance of KeyGen

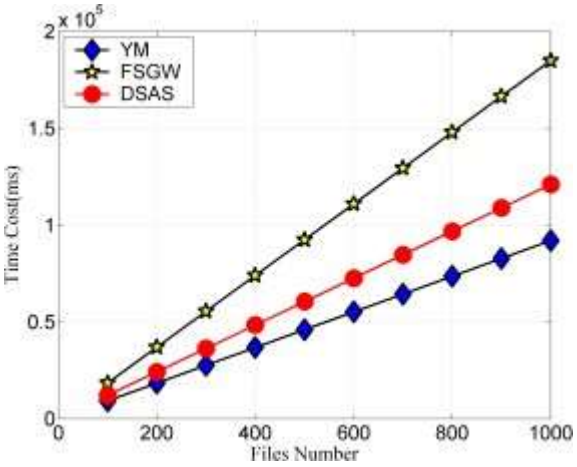

Fig 3: Performance of encrypt

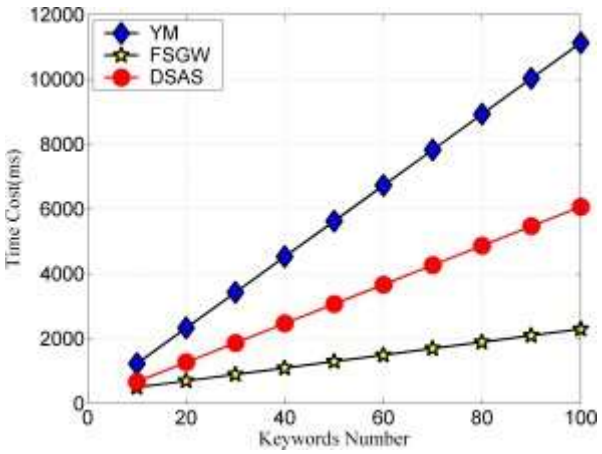

Fig 4: Performance of index encrypt.

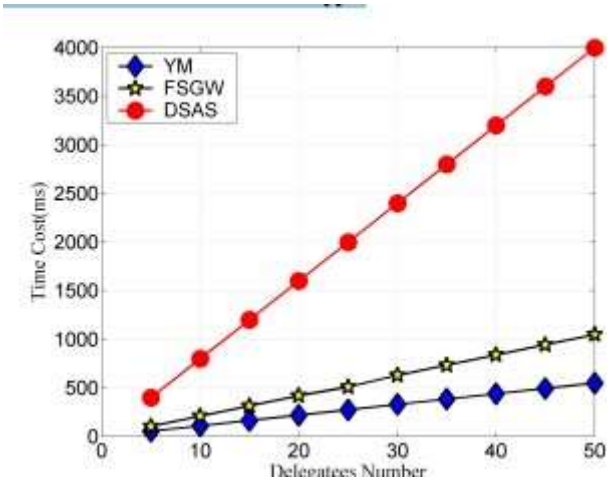

Fig 5; . Performance of ReKeyGen.

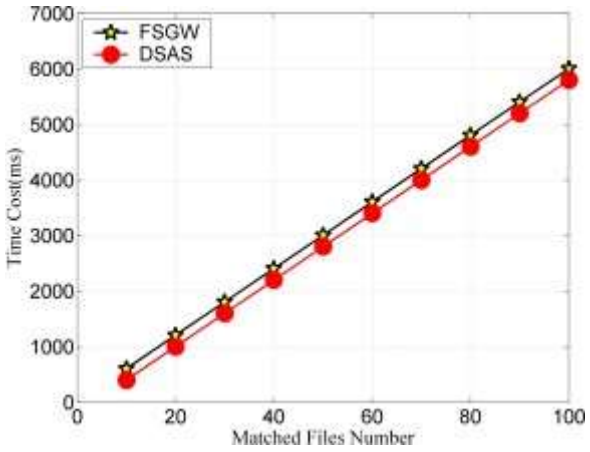

Fig 6: Performance of decrypt.

By embracing the Sort A bends inside the Paring Based Cryptography (PBC) library [22], we play out our proposed conspire on a PC with 1.8-GHz Intel Center processor i5-8250U (Window 10 activity framework, and a Slam of 8 GB) to go about as the cloud server. This reproduction climate is utilized to perform calculations ReEnc and Test, which require an extraordinary computational and stockpiling capacity. To perform the algorithms KeyGen, Enc, ReKeyGen, Trapdoor, and Dec, we deploy two Raspberry Pi sensor nodes (ARM Cortex-A53 1.2GHz 64-bit quad-core ARMv8 CPU) to form a wirelessly linked Industrial Internet of Things (IIoT). In contrast, the users or sensor devices in our system require low computational capability. The hubs speak with one another by ZigBee convention. The sensor hubs speak with the cloud server through one-bounce or multihop way. Let |G| denote the bit length of a G element, and let |GT| denote the bit length of a GT element in the experiment. Because only

FSGW [12] and YM [46] are about conditional searchable proxy re encryption, we only compare our scheme to these two. The simulation results are shown in Figure. 2 to Fig. 6.

5. CONCLUSION

In this paper, we introduced an intermediary imperceptible condition-concealing intermediary re-encryption plot which upholds catchphrase search that can be applied to getting information sharing and designation in e-medical care frameworks. By specifying a re-encryption key, a doctor named Alice (the delegator) can use our new system to create a conditional authorization for a doctor named Bob (the delegate). The cloud server can per-form cipher text transformation with the re-encryption key, allowing Bob to access the original encrypted file under Alice's public key and enabling secure delegation. The doctor's encrypted patient records can be searched on behalf of the cloud server without the doctor knowing anything about the keyword or the underlying condition. In particular, we were successful in achieving the system-invisible proxy property. We have likewise gotten the property of plot opposition in the framework, where a delegator's (Alice) confidential key is as yet secure even an unscrupulous cloud server conspires with the representative (Bounce). We have shown security through a thorough verification, and the exhibition examination affirms that our proposed plot DSAS is proficient and functional.

REFERENCES

[1] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange,

J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, ``Searchable encryption

Revisited: Consistency properties, relation to anonymous IBE, and exten-

Sions," in Proc. Annu. Int. Cryptol. Conf. Berlin, Germany: Springer, 2005,

Pp. 205_222.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, ``Improved proxy re-

Encryption schemes with applications to secure distributed storage," ACM

Trans. Inf. Syst. Secur., vol. 9, no. 1, pp. 1_30, 2006.

[3] J. Baek, R. Safavi-Naini, and W. Susilo, ``Public key encryption with

Keyword search revisited," in Proc. Int. Conf. Comput. Sci. Appl. (ICCSA),

2008, pp. 1249_1259.

[4] T. Bhatia, A. K. Verma, and G. Sharma, ``Towards a secure incremental

Proxy re-encryption for e-healthcare data sharing in mobile cloud com-

Puting," Concurrency Comput., Pract. Exper., vol. 32, no. 5, p. E5520,

Mar. 2020.

[5] T. Bhatia, A. K.Verma, and G. Sharma, ``Secure sharing of mobile personal

Healthcare records using certi_cateless proxy re-encryption in cloud,"

Trans. Emerg. Telecommun. Technol., vol. 29, no. 6, p. E3309, Jun. 2018.

[6] I. F. Blake, G. Seroussi, and N. Smart, ``Advances in Elliptic Curve

Cryptography (London Mathematical Society Lecture Note Series (317)),

Vol. 19. Cambridge, U.K.: Cambridge Univ. Press, no. 20, 2005, p. 666.

[7] M. Blaze, G. Bleumer, and M. Strauss, ``Divertible protocols and atomic

Proxy cryptography," in Advances in Cryptology-EUROCRYPT. Berlin,

Germany: Springer, 1998, pp. 127_144.

[8] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, ``Public

Key encryption with keyword search," in Proc. Int. Conf. Theory Appl.

Cryptograph. Techn. Berlin, Germany: Springer, 2004, pp. 506_522.

[9] D. Boneh and B. Waters, ``Conjunctive, subset, and range queries on

Encrypted data," in Proc. Theory Cryptogr. Conf. Berlin, Germany:

Springer, 2007, pp. 535_554.

[10] H. Fang, X. Wang, and L. Hanzo, ``Learning-aided physical layer authen-

Tication as an intelligent process," IEEE Trans. Commun., vol. 67, no. 3,

Pp. 2260_2273, Mar. 2019.

[11] H. Fang, L. Xu, and X. Wang, ``Coordinated multiple-relays based

Physical-layer security improvement: A single-leader multiple-followers

Stackelberg game scheme," IEEE Trans. Inf. Forensics Security, vol. 13,

No. 1, pp. 197_209, Jan. 2018. [12] L. Fang, W. Susilo, C. Ge, and J. Wang, ``Chosen-ciphertext secure

Anonymous conditional proxy re-encryption with keyword search," Theor.

Comput. Sci., vol. 462, pp. 39_58, Nov. 2012.

[13] L. Fang, J. Wang, C. Ge, and Y. Ren, ``Fuzzy conditional proxy re-

Encryption," Sci. China Inf. Sci., vol. 56, no. 5, pp. 1_13, May 2013.

[14] J. Feng, L. T. Yang, R. Zhang, W. Qiang, and J. Chen, ``Privacy preserv-

Ing high-order bi-Lanczos in cloud-fog computing for industrial appli-

Cations," IEEE Trans. Ind. Informat., early access, May 28, 2020, doi:

10.1109/TII.2020.2998086.

[15] J. Feng, L. T.Yang, Q. Zhu, and K.-K.-R. Choo, ``Privacy-preserving tensor

Decomposition over encrypted data in a federated cloud environment,"

IEEE Trans. Dependable Secure Comput., vol. 17, no. 4, pp. 857_868,

Jul. 2020.

[16] J.-S. Fu, Y. Liu, H.-C. Chao, B. K. Bhargava, and Z.-J. Zhang, ``Secure

Data storage and searching for industrial iot by integrating fog comput-

Ing and cloud computing," IEEE Trans. Ind. Informat., vol. 14, no. 10,

Pp. 4519_4528, Oct. 2018.

[17] M. Green and G. Ateniese, ``Identity-based proxy re-encryption," in

Applied Cryptography and Network Security. Berlin, Germany: Springer,

2007, pp. 288_306.

[18] D. He, M. Ma, S. Zeadally, N.Kumar, and K. Liang, ``Certi_cateless public

Key authenticated encryption with keyword search for industrial Internet

Of Things," IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3618_3627,

Aug. 2018.

[19] Y. J. He, T. W. Chim, L. C. K. Hui, and S.-M. Yiu, ``Non-transferable

Proxy re-encryption scheme for data dissemination control," IACR Cryp-

Tol. Eprint Arch., vol. 2010, p. 192, Jan. 2010.

[20] Q. Huang, L. Wang, and Y. Yang, ``Secure and privacy-preserving

Data sharing and collaboration in mobile healthcare social networks

Of smart cities," Secur. Commun. Netw., vol. 2017, pp. 1_12,

Aug. 2017.

[21] Q. Huang, Y. Yang, and J. Fu, ``PRECISE: Identity-based private data

Sharing with conditional proxy re-encryption in online social networks,"

Future Gener. Comput. Syst., vol. 86, pp. 1523_1533, Sep. 2018.

[22] B. Lynn. (2006). PBC Library. [Online]. Available: http://crypto.

Stanford.edu/pbc

[23] M. Ma, D. He, D. Kumar, K.-K. R. Choo, and J. Chen, ``Certi_cateless

Searchable public key encryption scheme for industrial Internet of Things,"

IEEE Trans. Ind. Informat., vol. 14, no. 2, pp. 759_767, May 2017.

[24] Y. Miao, J. Ma, X. Liu, F. Wei, Z. Liu, and X. A. Wang, ``m2-ABKS:

Attribute-based multi-keyword search over encrypted personal health

Records in multi-owner setting," J. Med. Syst., vol. 40, no. 11, p. 246,

Nov. 2016.

[25] M. Naz, F. A. Al-zahrani, R. Khalid, N. Javaid, A. M. Qamar, M. K. Afzal,

And M. Sha_q, ``A secure data sharing platform using blockchain and

Interplanetary _le system," Sustainability, vol. 11, no. 24, p. 7054, 2019.

AUTHOR PROFILE

Mr. K. Jaya Krishna Associate Professor in the department of MCA at QIS college of engineering and technology. He is having over 20 research publication. His area of interest is Machine Learning and Cloud Computing.

Mr.M.V.Ranga Reddy PG Scholar in the department of MCA, QIS College of engineering and Technology(Autonomous), Vengamukkapalem, Prakasam(DT) His areas of Interests are Networking & Cloud Computing.