International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Research Analysis on Encryption Algorithms for Cloud Authentication in Hms

Ananya K, Jahanara Khanam, Santhosh Kumar B J

Abstract: ***With the advancement of Internet of Things, mutual sharing of data turns out to be simple among different brilliant gadgets over the globe. In such a situation, a smart health care should be accelerated with a goal to provide a secure patient's record situated globally. In any case, as the sensitive data about a patient passes through an open channel (i.e., the Internet), there are odds of abusing this data and intercepting message communication and possibility of passive attack. These attacks are undetected and unavoidable over open channels. Thus, there is a necessity for a solid crypto system for safely handling keen human services information. To ensure that the patients' right over their own information, it is a assuring technique to scramble the information's by the time it gets re-appropriated. We are presenting a secure data retrieval scheme by comparing various algorithms that manage their attributes independently. The proposed application mainly insist on current attribute based encryption mechanism and providing compared efficiency.***

Keywords: ***Algorithms: ABE, IBE, CPABE, encryption. decryption, access control, security.***

I. INTRODUCTION

The cloud computing is the act of storing away consistently utilized information on various servers that can be sent or received through the Internet. The "cloud" is made out of hardware, storage, networks, interfaces, and services, interfaces, and administrations that give the methods through which clients can get to the frameworks, processing force, applications, and administrations on interest which are autonomous of areas. Now s days ,the healthcare sectors are given with more security and the details of the patient health reports must be securely stored on a cloud. It has become one of the important issues of sharing the data online. The model that emerges from the idea of giving security must satisfy the security concerns like make, manage the details of the patient's reports that is stored and retrieved online efficiently. The major goal of any health sector is to provide the opportunity of giving the accessibility of the user's data among many people and the services to many. In order to make the health sector more secure with the services, the quality can be increased by the feature of assessment of a large number of data that is functioning and upgraded in that environment. The cloud environment enhances the patient concern by giving various well planned services which can be reached to the user in a faster way and in an efficient manner with less budget, hence meet the goal of the health sector. The outcome of this brings in moving the information in the system to the cloud and the remote user's can make use of this in any geographical boundaries. The access to the data can be done by the respective doctor's even they are located in distant places. There is no need of the direct connect between the physicians instead they can get the information from the cloud. Social insurance conditions require a foundation which decreases tedious endeavours and exorbitant activities to acquire a patient's finished therapeutic record and consistently coordinates gathered of medical information to convey it to the human services experts. Distributed computing condition enhances tolerant consideration by giving better, quicker, more secure and all inclusive administrations at a lower cost and which meets the prerequisites of the medical service area. So the medicinal services suppliers are all the more eager to move their frameworks to the mists that can expel the topographical separation hindrances among social insurance suppliers and patients. With distributed computing, distinctive specialists can get to a patient's wellbeing records, regardless of whether they're miles separated. These doctors require not have an immediate correspondence to ask for an exchange of wellbeing records. They can simply get to them through the mists. The members of the health management can be given guarantees to the information of the patient. The security ought to be given on the patient information and to explicit specialists. If the server side is not sure about the client then it would be difficult to create a secure cloud on a public cloud.

However, the sensitive details of the patient's on cloud leads to significant security and privacy issues, so that they can attack by the third party. The subjection of those leaked information may cause the misapplication of the patient's details and cause problem in their medicine. Hence, the data used by the unauthorized user must be controlled by providing an efficient system. The information must be encrypted firstly, then it should be fed to the storage in order to avoid attacks. So, a well built mechanism should be found out for healthcare sector and maintain privacy.

II. RELATED WORK

The literature of cloud based authentication is mostly related to works in the cryptographic area and the principles of attribute based encryption using which any access to the data can be achieved for the data which is outsourced. To ensure the proper usage of data the various encryption algorithms have been used and the effective usage of the key and their management is done. Several keys are used to improve the expandable solutions and usage of different user's key. ABE us used in a proper way under a given set of attributes, encryption can be done through this set of attributes and owns proper keys.

Revised Manuscript Received on 30 July 2019.

***** Correspondence Author

Ananya K*, Department of Computer science, Amrita School of Arts and Sciences, Mysuru, Amrita Vishwa Vidyapeetham, India

Jahanara Khanam, Department of Computer science, Amrita School of Arts and Sciences, Mysuru, Amrita Vishwa Vidyapeetham, India

Santhosh Kumar B J, Department of Computer science, Amrita School of Arts and Sciences, Mysuru, Amrita Vishwa Vidyapeetham, India

This kind of feature makes the encryption process more efficient and the management of keys efficiently. The main advantage of ABE is to prevent user collusion.Secure user data in cloud computing using encryption algorithms are dealing with the issues we find in cloud on security, its composition and the designing challenges when building a secure cloud. The various calculations on algorithms and their results for distinctive worries with the consideration of the misfortune of information, segregation of the data and safeguarding them on the web Calculations like: [1] RSA, DES, AES, Blowfish have taken into consideration and the clear differences between them is observed in the ways of the quality of security they have provided. Based on the Encryption calculations that are made and comparisons between AES, DES, Blowfish and RSA are made and the best algorithm which gives security efficiently is chosen so that no third person can misuse it and providing a great security to the cloud. The personal health reports of the patient are given with a secure and scalable environment in the cloud by using an attribute based encryption algorithm In order to gain a fully efficient access and usage of the patient's details and control of the information the usage of attribute based encryption [2] is done. The encryption of the patient's records is done using the ABE algorithm. Basically, the owner of the record herself or himself must take decisions on the possible methods to encrypt the file and to whom all the access of the file should be given. The reports of the patient must be shared only to the users who have received the decryption key, while it remains confidential for the rest of the members. The electronic wellbeing record comprises of pictures of the patient's record which is extremely classified [3]. The Electronic Health Records in the human services division incorporates the sweep pictures, X-beams, DNA reports and so on., which are considered as the patients private information. It requires a high level of protection and verification. The symmetric cryptographic calculation named as Advanced Encryption Standard (AES) is used. An exploration on secure document stockpiling on cloud utilizing cryptography where it is to safely store data into the cloud, by part information into a few pieces and putting away parts of it on a cloud in a way that jelly information confidentiality , uprightness and guarantees accessibility. Utilizing AES, DES and RC2 calculation [4]. Enhances the execution amid encryption and unscrambling process.[5] Attribute based encryption provides a fine grained access control for the cloud. It helps in embracing the CP-ABE algorithm and makes it worth for all kinds of cloud environment for portable condition also and hence changes the structure of the cloud. ABE is an open key cryptography method that utilizes one-too-numerous encryption. ABE utilizes properties as personalities for both encryption and decoding of information.

[6] An exploration on Cloud figuring empowers the clients to store the information in a safe place and can be used whenever needed. A standout amongst the most ideal ways is CP-ABE is to take care of the difficult issue of secure information sharing plan in distributed computing. CP-ABE a modification of Attribute Based Encryption (ABE) for the purposes behind giving confirmations towards the province the sensitive data.[9] The data which should be securely stored and saved on a cloud can be authenticated by the identity based encryption. An efficient protocol is used as unique identity and through which the authentication can be given to the important information However the cyber attacks can be reduced by this mechanism. The protocol provides mutual authentication, a secure end to end communication. An exploration on Cryptographic Cloud Storage [8].The central properties of a system of cryptography is that in controlling of the information that is being given privacy by the client and the security features are gotten from the properties of cryptography, rather than legitimate components, the real time security and the control of accessibility. In (cipher text-approach) trait based encryption conspire every client in the framework is given an unscrambling key that has a lot of qualities related to it (this is the manner by which the "accreditations" in Section 2 would be actualized). A client would then be able to encode the message under a public key and a strategy.

III. DESCRIPTION ON COMMON ENCRYPTION ALGORITHMS:

a. Attribute Based Encryption:

The main goal of the ABE is to extend the security in a better way and the control of accessibility of the information among people using it. ABE is an efficient algorithm which uses public key and with the set of attributes values it does its encryption and decryption process efficiently. It takes the user data and the attribute set into main consideration to do the key generation to use when decrypting the data. Collusion resistance is the decisive aspect of the security in the process of encryption in attributes based encryption. The keys reflect a true access structure. The decryption is done if and only if the keys are satisfied. The problem with the attribute based encryption is that it's the person who does encryption does not know all the set of attributes to nullify and there may be chance of ending up with huge attributes. When the storage is a problem the loss of information will be less. There is no need of server that mediates the file instead the access policies must be well known and that is enough for the complete protection. The drawbacks of attribute based encryption can be its inefficiency and the coordination of the keys and the key escrow problem.

b. Cipher-Text Attribute Based Encryption:

CP-ABE was introduced Sahai, and it is the next version of attribute based encryption. CP-ABE works on the scheme that the cipher text is relates to the two major factors like the access policy that are given to the set of attributes and the next is that it should contain a private key which is also associated with that set of attributes. The decryption process happens only if the cipher text matches the policy that is linked with the set of attributes. If this match, then a user can decrypt the cipher text. It works on one-many encryption methods and provide a secure and flexible environment to the cloud authentication. It works in the opposite way of Key-Policy attribute based encryption. The one more feature of CPABE is that once the data is encrypted by satisfying the policies, the private keys can be shared among the users. So, the encryption can be done without taking policies into consideration, but the decryption is carried out only if the policies match.

c. Identity Based Encryption:

It is one of the prominent method of cryptography. It works on public keys and contains a unique identity for the identification. The distinctive identity can be considered as the key. ID-based encryption was introduced in1984 by Adi Shamir. The central authority generated the keys for all the user's, generally the secret keys and the distinctive identity are made in the process for example register number or the address. The server who has all access to those parameters of the system can encrypt the information using those parameters. Later the centralized one sends the key to the client. Identity Based Encryption has the rights in generating public keys and the private keys are generated from the main authority. This may lead to the key escrow problem. The IBE system can also reduce the infrastructure of the public key generation.

IV. COMPARISION OF CHARACTERISTICS OF ALGORITHM:

TABLE.1

Characteristics	***ABE***	***IBE***	***CPABE***
Platform	Cloud computing	Cloud computing	Cloud computing
Time of execution	54	28	9.89
Type of security	Less	moderate	more
Capacity of data encryption	256	256	3196
Authentication type	Less compared to CP-ABE	Better than ABE	More efficient
Memory usage	more	more	less

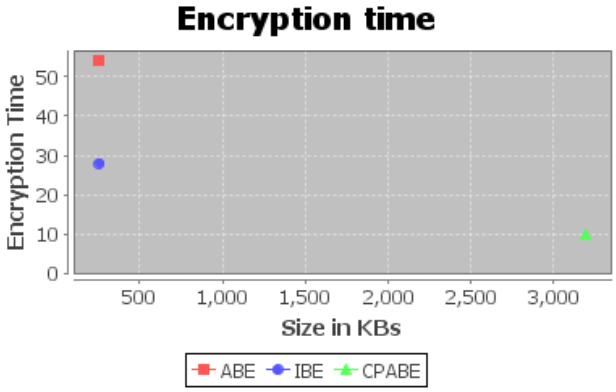

FIGURE.1

V. CONCLUSION AND FUTURE WORK:

The paper deals with the comparative study and analysis of various algorithms like to attribute based encryption, cipher-text attribute based encryption and identity based encryption. As the internet is extending tremendously over the world and the usage of it has increased in a great manner. Hence the security of the information we share over cloud must be given efficiently and prevent the misuse of information especially in the field of medicine. In order to provide security to the medical field data the various cryptographic algorithms are used and through them the reliability of information is achieved. In this paper, the characteristics of algorithms are shown in a production format and also observed that CP-ABE is more efficient and takes less time to process of encryption and decryption. The enhancement of the algorithms can be done in further work. The future work will be done in such a way a better security system would be built by using the efficient algorithms which results in more scalable and secure authenticated system for the storage and sharing of information.

REFERENCES

1. Arora, R., Parashar, A., & Transforming, C. C. I. (2013). Secure user data in cloud computing using encryption algorithms. *International journal of engineering research and applications*, *3*(4), 1922-1926.
2. Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE transactions on parallel and distributed systems*, *24*(1), 131-143.
3. Arunkumar, R. J., & Anbuselvi, R. (2017). Enhancement of cloud computing security in the health care sector. *International Journal of Computer Science and Mobile Computing*, *6*(8), 23-31.
4. Muthukumar, K. A., & Nandhini, M. (2016, March). Modified secret sharing algorithm for secured medical data sharing in cloud environment. In *2016 Second International Conference on Science Technology Engineering and Management (ICONSTEM)* (pp. 67-71). IEEE.
5. Guo, C., Zhuang, R., Jie, Y., Ren, Y., Wu, T., & Choo, K. K. R. (2016). Fine-grained database field search using attribute-based encryption for e-healthcare clouds. *Journal of medical systems*, *40*(11), 235.
6. Wang, Y., Sun, Q., Ma, Y., Zhang, J., Liu, Z., & Xue, J. (2018, June). Security Enhanced Cloud Storage Access Control System Based on Attribute Based Encryption. In *2018 International Conference on Big Data and Artificial Intelligence (BDAI)* (pp. 52-57). IEEE.
7. Manishankar, S., Arjun, C. S., & Kumar, P. A. (2017, June). An authorized security middleware for managing on demand infrastructure in cloud. In *2017 International Conference on Intelligent Computing and Control (I2C2)* (pp. 1-5). IEEE.
8. Mukhopadhyay, A., Suraj, M., Sreekumar, S., & Xavier, B. (2018, September). Emergency Healthcare Enhancement by Multi-Iterative Filtering of Service Delivery Centers. In *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 1581-1587). IEEE.
9. Karati, A., Amin, R., Islam, S. H., & Choo, K. K. R. (2018). Provably secure and lightweight identity-based authenticated data sharing protocol for cyber-physical cloud environment. *IEEE Transactions on Cloud Computing*.
10. Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H., & Tang, Y. (2018). Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. *Journal of Network and Computer Applications*, *106*, 117-123.
11. Jiang, Y., Susilo, W., Mu, Y., & Guo, F. (2018). Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing. *Future Generation Computer Systems*, *78*, 720-729.
12. Wang, Q., Peng, L., Xiong, H., Sun, J., & Qin, Z. (2018). Ciphertext-policy attribute-based encryption with delegated equality test in cloud computing. *IEEE Access*, *6*, 760-771.
13. Joshi, M., Joshi, K., & Finin, T. (2018). Attribute Based Encryption for Secure Access to Cloud Based EHR Systems. *UMBC Information Systems Department Collection*.
14. Zhao, B., Hu, L., Zang, Y., Liu, Y., Wen, X., & Li, H. (2018, May). Safe Cloud Storage of Medical Information Based on Attribute Encryption. In *2018 2nd International Conference on Applied Mathematics, Modelling and Statistics Application (AMMSA 2018)*. Atlantis Press.

15. Kumar, B. S., Raj, V. R., & Nair, A. (2017, April). Comparative study on aes and rsa algorithm for medical images. In *2017 International Conference on Communication and Signal Processing (ICCSP)* (pp. 0501-0504). IEEE.
16. Li, J., Li, J., Chen, X., Jia, C., & Lou, W. (2015). Identity-based encryption with outsourced revocation in cloud computing. *Ieee Transactions on computers*, *64*(2), 425-437.
17. Hu, G., Xiao, D., Xiang, T., Bai, S., & Zhang, Y. (2017). A compressive sensing based privacy preserving outsourcing of image storage and identity authentication service in cloud. *Information Sciences*, *387*, 132-145.

AUTHORS PROFILE

Ananya K, MCA(Masters of Computer Applications) , Amrita School of Arts & Sciences, Amrita Vishwa Vidyapeetham, Mysore, karnataka, India.

Jahanara Khanam, MCA(Masters of Computer Applications) , Amrita School of Arts & Sciences, Amrita Vishwa Vidyapeetham, Mysore, karnataka, India.

Santhosh Kumar B J, Asst. Professor , Department of Computer Sciences , Amrita School of Arts & Sciences, Amrita Vishwa Vidyapeetham, Mysore, karnataka, India.