International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-9 Issue-1, May 2020

Multi-Authority Secure Database for Enabling Authorized Encrypted Search with Privacy Preserving on Healthcare Databases

Satish T. Pokharkar, Manoj kumar Rawat

Abstract*: *Now a day's in medical field number of application's will develop for overcome the complexity of previous work. By using information technology and computer science provide various new techniques and medical equipment's has improved digitalization in healthcare sector. In existing system much more advancement is providing to overcome the time and money of patients and perform exact treatments and store patient's confidential records in securely but most important issues are security. To address the existing security issues to design and develop the proposed research work on security i.e. for patient's confidential health data records in database servers. Existing work during data transmission can only protect the patient's data records but they can't stop the insider attacks. In proposed research work, first implement front end security with the help of keylogging technique, second to store patient's confidential data in multiple data servers or chunks and to prevent the insider attacks and third and most important is access policy of search for encrypted data of multi-authority. The main contribution of this research work to assign patients data records in different chunks securely and applying the cryptosystems for security goals of a patient's confidential records. Especially, proposed work advantages of SHA hashing technique to perform each and every user for access of particular data records. This research work explores secure data storage and sharing using proposed AES 128 encryption algorithm and Role Base Access Control (RBAC) for secure data access scheme for end user. This work also carried out backup server approach it works like proxy storage server for ad hoc data recovery for all distributed data servers.

Keywords*: *Wireless network, user data privacy, Paillier encryption, Multi-authority, encrypted data search, forward security, SHA Algorithm, Hashing Functions, ABE (Attribute Based Encryption) etc.

I. INTRODUCTION

Information uprightness protection is the principle point of an information distribution center. It includes audition using TTP for unauthorized access. Proposed work implements protecting the data and regeneration of data if someone mishandles it. To overcome these issue data will have stored in proxy server temporary purpose. And these data will be user stored in the public and private sectors of the data server. Therefore, private server data has been securely save and only public server data will be used by the user [6]. Once any illegal alteration is made, the primary data in the private server will be recovered by the Proxy server and will be returned to the user. Data storage usually gives different redundancy configurations to users to keep the aspired balance among achievement including fault-tolerance. Data availability is crucial in distributed storage policies, particularly when node failures remain common in real life. This research work explores secure data storage and sharing using proposed AES 256bit encryption algorithm and Role Base Access Control (RBAC) for secure data access scheme for end user. This work also carried out backup server approach it works like proxy storage server for ad hoc data recovery for all distributed data servers. The experiment analysis has proposed in public as well as private server storage environment. The most straight forward method is cryptosystem which is first encrypt data i.e. to convert plain-text to cipher-text and then upload it. In that SHA algorithm as well as Paillier cryptosystem are distribute user's data in multiple chunks and also store at proxy server for backup and recovery purpose. Finally, those users who have an access key of the data record can only that authorized user decrypt and access the data records.

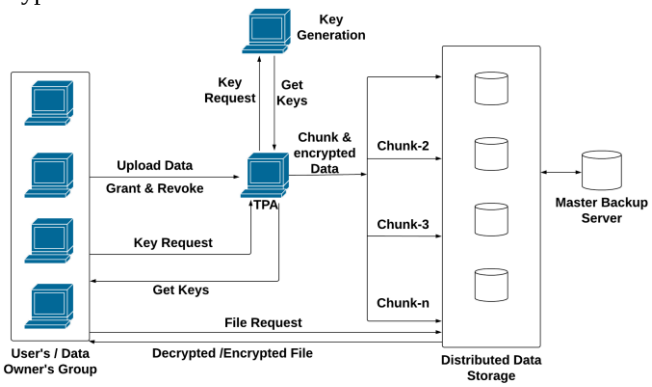

Fig.1: System Overview

In this research work the most important module is front end security. So, for frontend security use keylogging technique in healthcare application. In that keylogging technique, this is to avoid phishing attacks to the application of password security.

Manuscript received on April 02, 2020.
Revised Manuscript received on April 15, 2020.
Manuscript published on May 30, 2020.
* Correspondence Author
Satish Pokharkar*, Department of Computer Engineering, Oriental University, Indore, India. Email: satishpokharkar37@gmail.com
Dr. Manoj Kumar Rawat, Department of Computer Engineering, Oriental University, Indore, India. Email: drmkrawat@gmail.com

Therefore, healthcare application is more secure. Second thing is that data storage and accessibility. For this point use Secret Shamir hashing technique and keyword as well as content base cryptography techniques.

II. LITRATURE SURVEY

Now a day's there are number of information or data transmission continuously. So each and every time data will be convert in number of packet using IP Header format and send over a network. That's why main problem is that in data transmission there are number of unwanted packets also added during data transmission and also occurred unwanted traffic over network. Hence, in this work authors proposed A collaborative trust-based approach to reduce unwanted packets by using collaborative packet filtering approach and also reduce unwanted traffic and insider attacks over network [1]. In this paper, author propose a practical approach to prevent the inside attack in healthcare software defined network. In this proposed approach to detect the malicious healthcare devices in SDN's. That means paper proposed of only and only detection of unauthorized devices which is send malicious content by intruders [2]. In this paper authors use oLFSR and oXOR, to presenting an all-optical stream cipher (oSC). By using these techniques for security challenges stream cipher can have categorized the different guessing attacks in network. In this work authors proposed there are different attacks on the network during data transmission in that they only categorized guessing attacks on data packets [3]. In existing work Text-based Captchas are used but text-based captchas in that attack speed are moderate so this is not a secure technique so authors proposed new techniques which is image-based captchas but in this technique also an issues to manually select source images or add labels to images means it's a time consuming and not that much securely system that's why in this paper they propose Style Area Captcha (SACaptchas). In this scheme use different style area on selected image [4]. Recently, Structured Query Language (SQL) Injection Attack is major attacks it will leaks the confidential information. This attack is directly target on database because user will handle web or android application in remote location, so intruder attack on database and leak confidential data i.e. remove the parameters values of SQL query. So in this proposed work authors will design new techniques to detection of SQL Injection attacks [5].

III. RELATED WORK

Now a day's security is an important issue nowadays 99% of data process online and stored in trusted server. But when user store their data in authorized server they must be a data transmit and receive through secure communication channel and that time security issue are occurred. Recently, maximum data are process in following applications or fields.

- Healthcare
- E-Commerce
- Internet Baking
- Education and
- Business application etc.

These all are services are used over internet and number of chances for various attacks in online services. To address these issue's use access policy, dynamic authentication method, and keylogging security service as a security from various attacks. Here these all techniques are based on human behavior to recognize their action. As the dynamics password no need any external hardware components only for using software-based system can achieve security of data records [7]. In existing work can only detect various attacks like, guessing attack, SQL Injection attack, password based attacks, and malicious devices in SDN but these all system can't anyone stop the attacks which effects on user's data records [5]. So, in this proposed research work to address all these issue and overcome the attacks detection and prevention techniques.

A. System Architecture:

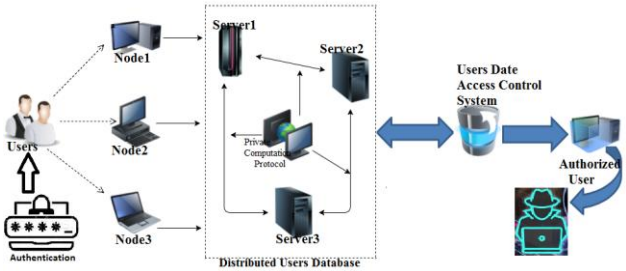

Fig.2: System Architecture

B. Multi-Authority:

In this research work support search capability in which all data records which already stored in database with different chunks. In this work main aim is that to search data which is encrypted at the time of upload. Multi-authority means that the data records all authorities can allocate their searching ability to user as well as clients which is supporting various authorities. With the help of Aspect based encryption technique to improve searching capability [8].

C. Access Policy:

In that to provide access for that user which is a part of the system. Using attribute or aspect-based encryption provides various searching ability for different keywords which is encrypted with access policy of different user searching skills. In proposed work provide various parameters for access policy of different users with users searching skills and authorized access key.

D. Fine-Grained Access Control

In this system using access or secret key client can allow to decrypt the encrypted data records under certain access policies. These all work comes under an attribute or aspect-based encryption scheme. To improve the scalability and efficiency of access policy use cipher-text policy ABE and attribute or aspect-based encryption are classified in a couple of distinct role which are CP-ABE and KP-ABE [9].

E. Front-End Security (Keylogging Technique)

Keylogging or keyboard capturing is the activity of recording the keys struck on a keyboard, usually in a secretive mode so that each individual employing this keyboard is inattentive that their movements are being examined. In this research work get use keylogging technique for overcome the keylogging attack and provide better security of our application front end or login page.

In that password will set at the time of registration and login time it will use with the help of calculator keypad script and it will hide of password which is different combination of random number and access by OTP and keystroke event [10].

IV. RESULTS AND DISCUSSION

In this research work is implement a web-based application for healthcare community to prevent various attacks of patients as well as user's confidential data records storage and transmission time. The result analysis is done on the basis of following parameters is as follows:

- Time consumption
- Response Time
- Computation Cost
- Performance accuracy

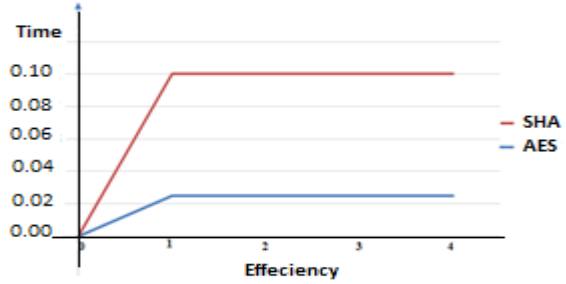

Fig.3: Time and Efficiency Chart

Here, Whole System took many more attributes for the input purpose but here mainly focuses on the Time and performance of the system. Based on some few attributes we will get the following analytical result for our proposed system.

Parameter	Existing	Proposed
A	10	4
B	10	5
C	8	8
D	10	3
E	8	2

Table 1: Result Table

Where,

A = Time Consumption.

B = Response Time.

C = Computation Cost.

D = Performance accuracy

E = Scalable & User Friendly.

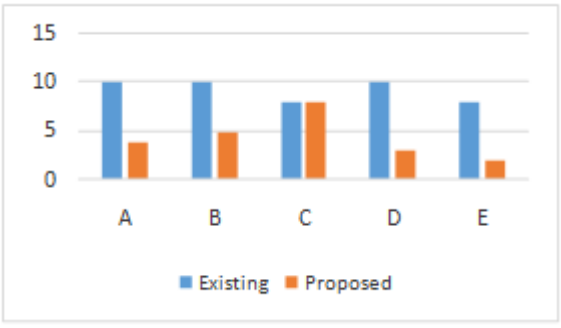

Fig.4: Time line chart of Result Analysis

V. CONCLUSION

In this article propose a secure database accessibility using an effective technique of encrypted data searching ability for multi-authority healthcare databases. In this research first phase work, get use of keylogging technique for overcome the keylogging attack and provide better security of our application front end or login page. Second phase work, implements protecting the data and transformation of data if the unauthorized user mishandles it. In third phase work, also provide a statistical approach at database security is a store data in different data chunks with AES encryption techniques as well as SHA hashing algorithm. Fourth phase work, secure attribute-based encryption technique for a multi-authority data access scheme on protecting patient's confidential data records. In this manner to provide practical approach for store, access and data transmission in any remote system and online healthcare networks etc.

ACKNOWLEDGMENT

I am grateful to all of those with whom I have the pleasure to work during this and other related projects. I thankful to my guide Dr. Manojkumar Rawat sir and Dr. R. K. Jain Dean of University have provided me extensive personal and professional guidance and taught me a great deal about the research. I especially thankful to computer department in oriental university for providing the resources.

REFERENCES

1. Weizhi Meng, Wenjuan Li, and Lam Kwok, "Towards Effective Trust-Based Packet Filtering in Collaborative Network Environments," IEEE Transactions on Network and Service Management, vol. 14, No.1, 2017
2. W. Meng, Kim-Kwang Raymond Choo, Steven F, Athanasios V. Vasilakos, and Christian W., "Towards Bayesian-based Trust Management for Insider Attacks in Healthcare Software-Defined Networks, "Future Generation Computer Systems, vols. 4344, pp. 99-109, 2015.
3. A. Engelmann and A. Jukan, W. zu Braunschweig, "Towards All-Optical Layered Encryption: A Feasibility Analysis of Optical Stream Cipher," IEEE Transactions on Information Forensics and Security, vol. 24, no. 1, pp. 131–143, 2019.
4. M. Tang, Haichang Gao, Yang Z, Yi Liu, Ping Zhang and P. Wang, "Research on Deep Learning Techniques in Breaking Text-based Captchas and Designing Image-based Captcha," IEEE Transactions on Information Forensics and Security, Vol.14, No.8, 2016.
5. Jose Fonseca, Marco Vieira, and Henrique Madeira, "Evaluation of Web Security Mechanisms Using Vulnerability & Attack Injection," IEEE Transactions on Dependable and Secure Computing, Vol. 11, No. 5, 2014.
6. Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," IEEE Communications Surveys and Tutorials, vol. 15, no. 2, pp. 1–17, Jul. 2012.
7. R. Wu, G.-J. Ahn, and H. Hu, "Secure sharing of electronic health records in clouds," In 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Work sharing (CollaborateCom), 2012, pp. 711-718
8. M. Shucheng Yu, Yao Zheng, Kui R., W. Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," IEEE Transactions on Parallel and Distributed Systems. Vol. 24, No. 1, 2013.
9. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing," in Proceedings of the IEEE INFOCOM, March 2010, pp. 1-9

10. DaeHun Nyang, Aziz Mohaisen, Jeonil Kang, “Keylogging-resistant Visual Authentication Protocols,” IEEE Transactions on Mobile Computing, vol. 1, no. 8, August 2014.

AUTHORS PROFILE

Mr. Satish Tukaram Pokharkar,
Student of Computer Department
Oriental University, Indore
Indore, India
Presently working as Assistant professor in SCSCOE Ahmednagar, Maharashtra, India of Computer Department Completed BE in north of Maharashtra University Jalgaon and M. Tech in RGPV Bhopal. I have more than 8 years of teaching experience and Published around 20 papers and attended many workshops and conferences.

Dr. Manoj kumar Rawat.
Professor of Computer Department,
Oriental University, Indore
Indore, India
Presently working as professor of CSE. Having more than 20 years of teaching and administrative experience at different university and colleges. Completed B. E, M. Tech Software Engineering from MNNIT, Allahabad and PhD in n CSE. Published around 30 papers and attended many workshops and conferences.