# Multi-Authority Secure Database for EnablingAuthorized Encrypted Search with Privacy Preserving on Healthcare Databases

**Juttiga Chandra Kumar[1], M Durga Rao[2]**

[1]*M.Tech Student, Department of CSE, Sri Vishnu Institute of Technology*
[2]*Assistant Professor, Department of CSE, Sri Vishnu Institute of Technology*

---

**ABSTRACT:** E-clinical statistics are touchy and need to be saved in a clinical database in encrypted form. However, clearly encrypting those statistics will do away with facts software and interoperability of the prevailing clinical database machine due to the fact encrypted statistics are not searchable. Moreover, more than one government can be worried in controlling and sharing the non-public clinical statistics of customers. However, authorizing distinctive customers to look and get entry to statistics originating from more than one government in a stable and scalable way is a nontrivial matter. To deal with the above issues, we advocate a licensed searchable encryption scheme below a multi-authority setting. Specifically, our proposed scheme leverages the RSA feature to permit every authority to restrict the hunt functionality of various customers primarily based totally on customers' privileges. To enhance scalability, we make use of multi-authority attribute-primarily based totally encryption to permit the authorization procedure to be accomplished best as soon as even over guidelines from more than one government. We behavior rigorous safety and price analysis, and carry out experimental critiques to illustrate that the proposed scheme introduces mild overhead to present searchable encryption schemes..

**Keywords: Wireless network, individual statistics privacy, Paillier encryption, Multi-authority, encrypted statistics search, beforehand safety, SHA Algorithm, Hashing Functions, ABE (Attribute Based Encryption) etc.**

## I. INTRODUCTION

Information uprightness safety is the precept factor of an statistics distribution center. It consists of audition the usage of TTP for unauthorized get right of entry to. Proposed paintings implements defensive the information and regeneration of information if a person mishandles it. To triumph over those difficulty information could have saved in proxy server brief purpose. And those information may be person saved withinside the public and personal sectors of the information server. Therefore, non-public server information has been securely shop and best public server information may be utilized by the person [6]. Once any unlawful alteration is made, the number one information withinside the non-public Revised Manuscript Received on May 01, 2020.

Server may be recovered via way of means of the Proxy server and may be back to the person. Data garage typically offers distinct redundancy configurations to customers to maintain the aspired stability amongst success along with fault-tolerance. Data availability is important in dispensed garage policies, specifically while node screw ups stay not unusualplace in actual life. This studies paintings explores stable information garage and sharing the usage of proposed AES 256bit encryption set of rules and Role Base Access Control (RBAC) for stable information get right of entry to scheme for quit person. This paintings additionally finished backup server method it really works like proxy garage server for advert hoc information healing for all dispensed information servers. The test evaluation has proposed in public in addition to non-public server garage environment. The maximum clear-cut technique is cryptosystem that's first encrypt information i.e. to transform plain-textual content to cipher-textual content after which add it. In that SHA set of rules in addition to Paillier cryptosystem are distribute person's information in more than one chunks and additionally keep at proxy server for backup and healing purpose. Finally, the ones customers who've an get right of entry to key of the information report can best that legal person decrypt and get right of entry to the information data.

In this studies paintings the maximum essential module is the front stop safety. So, for frontend safety use keylogging method in healthcare utility. In that keylogging method, that is to keep away from phishing assaults to the utility of password safety. Therefore, healthcare utility is extra stable. Second aspect is that statistics garage and accessibility. For this factor use Secret Shamir hashing method and key-word in addition to content material base cryptography strategies.

## II. LITRATURE SURVEY

Now a day's there are range of facts or statistics transmission continuously. So every and whenever statistics may be convert in range of packet the usage of IP Header layout and ship over a community. That's why fundamental trouble is that during statistics transmission there are range of undesirable packets additionally delivered for the duration of statistics transmission and additionally came about undesirable site visitors over community. Hence, on this paintings authors proposed A collaborative trust-primarily based totally technique to lessen undesirable packets through the usage of collaborative packet filtering technique and additionally lessen undesirable site visitors and insider assaults over community [1]. In this paper, creator recommend a sensible technique to save you the internal assault in healthcare software program described community. In this proposed technique to hit upon the malicious healthcare gadgets in SDN's. That approach paper proposed of best and best detection of unauthorized gadgets that's ship malicious content material through intruders [2]. In this paper authors use oLFSR and oXOR,

to offering an all-optical circulate cipher (oSC). By the usage of those strategies for safety demanding situations circulate cipher may have categorised the specific guessing assaults in community. In this paintings authors proposed there are specific assaults at the community for the duration of statistics transmission in that they best categorised guessing assaults on statistics packets [3]. In current paintings Text-primarily based totally Captchas are used however text-primarily based totally captchas in that assault velocity are slight so this isn't a stable method so authors proposed new strategies that's image-primarily based totally captchas however on this method additionally an troubles to manually choose supply pics or upload labels to pics approach it's a time eating and now no longer that a good deal securely device that's why on this paper they recommend Style Area Captcha (SACaptchas). In this scheme use specific fashion vicinity on decided on image [4]. Recently, Structured Query Language (SQL) Injection Attack is primary assaults it's going to leaks the personal facts. This assault is immediately goal on database due to the fact consumer will take care of net or android utility in faraway location, so intruder assault on database and leak personal statistics i.e. take away the parameters values of SQL query. So on this proposed paintings authors will layout new strategies to detection of SQL Injection assaults [5].

## III. RELATED WORK

Now a day's safety is an essential problem in recent times 99% of statistics system on-line and saved in depended on server. But whilst consumer shop their statistics in legal server they should be a statistics transmit and acquire thru stable communique channel and that point safety problem are came about. Recently, most statistics are system in following packages or fields.

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

These all are offerings are used over net and range of probabilities for diverse assaults in on-line offerings. To cope with those problem's use get right of entry to policy, dynamic authentication method, and keylogging safety carrier as a safety from diverse assaults. Here those all strategies are primarily based totally on human conduct to apprehend their action. As the dynamics password no want any outside hardware additives best for the usage of software program-primarily based totally device can attain safety of statistics records

[7]. In current paintings can best hit upon diverse assaults like, guessing assault, SQL Injection assault, password primarily based totally assaults, and malicious gadgets in SDN however those all device can't anybody forestall the assaults which results on consumer's statistics records [5]. So, on this proposed studies paintings to cope with these kinds of problem and conquer the assaults detection and prevention strategies.

### A. System Architecture:

**Multi-Authority:** In this studies paintings aid seek functionality wherein all facts facts which already saved in database with distinctive chunks. In this paintings foremost purpose is that to look facts that's encrypted on the time of upload. Multi-authority method that the facts facts all government can allocate their looking capacity to consumer in addition to customers that's assisting numerous government. With the assist of Aspect primarily based totally encryption method to enhance looking functionality [8].

**Access Policy:** In that to offer get admission to for that consumer that's part of the device. Using characteristic or aspect-primarily based totally encryption presents numerous looking capacity for distinctive key phrases that's encrypted with get admission to coverage of various consumer looking abilties. In proposed paintings offer numerous parameters for get admission to coverage of various customers with customers looking abilties and certified get admission to key. Control In this device the use of get admission to or mystery key purchaser can permit to decrypt the encrypted facts facts beneathneath sure get admission to policies. These all paintings comes beneathneath an characteristic or aspect-primarily based totally encryption scheme. To enhance the scalability and performance of get admission to coverage use cipher-textual content coverage ABE and characteristic or aspect-primarily based totally encryption are labeled in multiple wonderful position that are CP-ABE and KP-ABE [9].

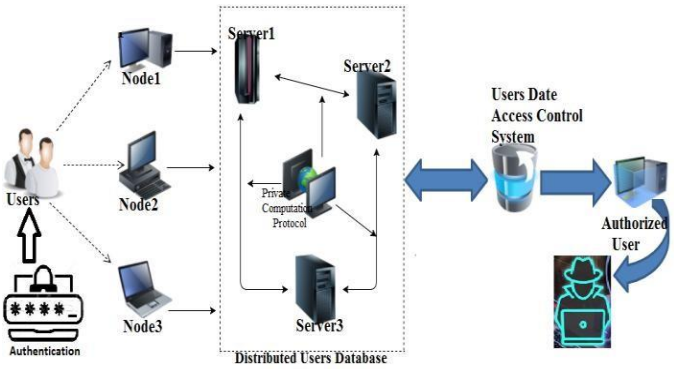


**Fig.1: System Architecture**

D. Front-End Security (Keylogging Technique) Keylogging or keyboard shooting is the interest of recording the keys struck on a keyboard, typically in a secretive mode so that every man or woman using this keyboard is inattentive that their actions are being examined. In this studies paintings get use keylogging method for triumph over the keylogging assault and offer higher protection of our utility the front stop or login page. In that password will set on the time of registration and login time it's going to use with the assist of calculator keypad script and it's going to conceal of password that's distinctive mixture of random range and get admission to through OTP and keystroke event [10]. I. RESULTS AND DISCUSSION In this

studies paintings is put in force a web-primarily based totally utility for healthcare network to save you numerous assaults of sufferers in addition to consumer's exclusive facts facts garage and transmission time. The end result evaluation is accomplished on the idea of following parameters is as follows:

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

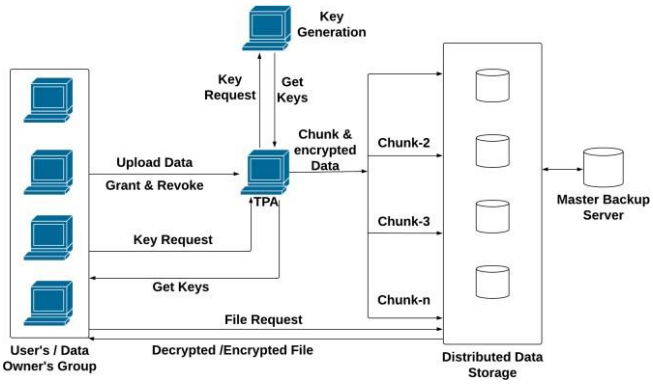


**Fig.2: System Overview**

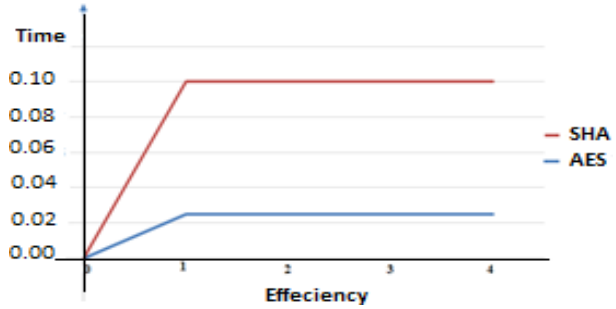


**Fig.3: Time and Efficiency Chart**

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**

## IV. CONCLUSION

In this paper, we gift a sensible and green legal encrypted seek scheme for multi-authority scientific databases, and it additionally helps ahead security. Our creation is L-adaptive-stable with the designed leakage functions, that are additionally non-interactive. The proposed device suggests a way to construct a fine-grained encrypted database seek device for a couple of authorities. In addition, we additionally gift an evaluation of our framework houses. There are a few thrilling open issues that deserve in addition investigation, inclusive of, designing greater realistic Boolean question searchable encryption with ahead security, exploiting the approach of simplifying get admission to manage for information proprietors or customers etc.

## V. REFERENCES

[1] J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: Ciphertext-policy attributebased signcryption," Future Generation Comput. Syst., vol. 52, pp.67–76, 2015.

[2] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, 2013.

[3] Y. Zhang, J. Katz, and C. Papamanthou, "All your queries are belong to us: The power of file-injection attacks on searchable encryption," in Proc. of 25th USENIX Secur. Symp., 2016, pp. 707–720.

[4] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," in Proc. of 36th Annu. Symp. on Foundations of Comput. Sci., 1995, pp. 41–50.

[5] X. Yuan, X. Wang, C. Wang, C. Qian, and J. Lin, "Building an encrypted, distributed, and searchable key-value

store," in Proc. Of the 11th ACM on Asia Conf. on Comput. and Commun. Security, 2016, pp. 547–558.

[6] S. Lai, S. Patranabis, A. Sakzad, J. K. Liu, D. Mukhopadhyay, R. Steinfeld, S.-F. Sun, D. Liu, and C. Zuo, "Result pattern hiding searchable encryption for conjunctive queries," in Proc. of the 2018 Conf. on Comput. and Commun. Secur. ACM, 2018, pp. 745–762.

[7] S.-F. Sun, X. Yuan, J. K. Liu, R. Steinfeld, A. Sakzad, V. Vo, and S. Nepal, "Practical backward-secure searchable encryption from symmetric puncturable encryption," in Proc. of the 2018 Conf. on Comput. and Commun. Secur. ACM, 2018, pp. 763–780.

[8] L. Xu, X. Yuan, C. Wang, Q. Wang, and C. Xu, "Hardening database padding for searchable encryption," in Proc. of the 2019 Conf. on Int. Conf. on Comput. Commun. IEEE, 2018.

[9] S. K. Kermanshahi, J. K. Liu, and R. Steinfeld, "Multi-user cloudbased secure keyword search," in Proc. of 22nd Aus. Conf. on Inf.Secur. and Privacy, 2017, pp. 227–247.

[10] X. Yang, T. Lee, J. K. Liu, and X. Huang, "Trust enhancement over range search for encrypted data," in Proc. of 2016 IEEE Trustcom/BigDataSE/ISPA, 2016, pp. 66–73.

[11] Z. Deng, K. Li, K. Li, and J. Zhou, "A multi-user searchable encryption scheme with keyword authorization in a cloud storage,"Future Generation Comput. Syst., vol. 72, pp. 208–218, 2017.

[12] S. Sun, J. K. Liu, A. Sakzad, R. Steinfeld, and T. H. Yuen, "An efficient non-interactive multi-client searchable encryption with support for boolean queries," in Proc. of 21st Eur. Symp. on Research in Comput. Secur., 2016, pp. 154–172.

[13] D. Cash, S. Jarecki, C. S. Jutla, H. Krawczyk, M. Rosu, and M. Steiner, "Highly-scalable searchable symmetric encryption with support for boolean queries," in Proc. of 33rd Annu. Cryptology Conf., 2013, pp. 353–373.

[14] X. Yuan, H. Cui, X.Wang, and C.Wang, "Enabling privacy-assured similarity retrieval over millions of encrypted records," in Proc. Of 20th Eur. Symp. on Research in Comput. Secur., 2015, pp. 40–60.

[15] X. Yuan, X. Wang, C. Wang, C. Yu, and S. Nutanong, "Privacypreserving similarity joins over encrypted data," IEEE Trans. Inf. Forensics Secur., vol. 12, no. 11, pp. 2763–2775, 2017.

[16] C. Zuo, J. Macindoe, S. Yang, R. Steinfeld, and J. K. Liu, "Trusted boolean search on cloud using searchable symmetric encryption," in Proc. of 2016 IEEE Trustcom/BigDataSE/ISPA, 2016, pp. 113–120. IEEE Transactions on Emerging Topics in Computing,Issue Date:18.March.2019.12

[17] S. Jarecki, C. S. Jutla, H. Krawczyk, M. Rosu, and M. Steiner, "Outsourced symmetric private information retrieval," in Proc .of 2013 ACM SIGSAC Conf. on Comput. and Commun. Secur., 2013, pp. 875–888.

[18] P. Xu, S. Liang, W. Wang, W. Susilo, Q. Wu, and H. Jin, "Dynamic searchable symmetric encryption with physical deletion and smallleakage," in Proc. of 22nd Aus. Conf. Inf. Secur. and Privacy, 2017,pp. 207–226.

[19] R. Bost, "Po'o&: Forward secure searchable encryption," in Proc.of the 2016 ACM SIGSAC Conf. on Comput. and Commun. Secur.,2016, pp. 1143–1154.

[20] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. of Int. Conf. on the Theory and Appl. of Cryptographic Tech., 2004, pp. 506–522.

[21] L. Fang,W. Susilo, C. Ge, and J.Wang, "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," Inf. Sci., vol. 238, pp. 221–241, 2013.

[22] L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage," IEEE Trans. Inf. Forensics Secur., vol. 8, no. 12, pp. 1947–1960, 2013.

[23] C. Zuo, J. Shao, Z. Liu, Y. Ling, and G. Wei, "Hidden-token searchable public-key encryption," in Proc. of 2017 IEEE Trustcom/ BigDataSE/ICESS, 2017, pp. 248–254.

[24] Y. Guo, X. Yuan, X. Wang, C. Wang, B. Li, and X. Jia, "Enabling encrypted rich queries in distributed key-value stores," IEEE Trans. on Parallel and Distrib. Syst., 2018.

[25] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. of 2007 IEEE Symp. on Secure. and Privacy, 2007, pp. 321–334.