International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

# An Advanced Healthcare System with IOT at its core and cloud support for safe, portable and accessible sharing of Information

**CH. SRI VALLI DHANA LAKSHMI**
Master of Computer Applications (MCA),
SVKP AND Dr.K.S Raju Arts & Science College(A),
Penugonda, W.G.Dt., A.P, India
srivalli7635@gmail.com

**B.N.Srinivasa Gupta**
Associate Professor in Computer Science,
SVKP AND Dr.K.S Raju Arts & Science College(A),
Penugonda, W.G.Dt., A.P, India
bnsgupta@gmail.com

## ABSTRACT :

Implementing a smart healthcare system that makes use of the Internet of Things (IoT) and the cloud is a new trend in healthcare information technology. Thanks to IoT-enabled and cloud-assisted healthcare technology, clinicians can monitor and respond to paroxysmal diseases in real time. Given the significance of patient privacy, it is critical that cloud-stored health data be encrypted to avoid unauthorised access by untrustworthy cloud firms and individuals. Encrypted health data stored in the cloud, on the other hand, makes retrieval more difficult for the data consumer. Furthermore, the tremendous computational demand stresses both the patient and physician sides' resource-constrained equipment. In this research, we present a lightweight attribute-based searchable encryption (LABSE) method for resource-constrained devices that enables fine-grained access control and keyword search while lowering computational cost. To address the healthcare scenario's security demands, we rigorously demonstrate the semantic security of the proposed LABSE scheme and examine other security concerns. Then, within the healthcare system, we construct a real LABSE deployment model. We compare LABSE to state-of-the-art equivalent systems in terms of usefulness and complexity. Finally, the experiment reveals the usefulness and performance benefits of the experiment.

**KEYWORDS :** Encrypted Data, Security Demands, Keyword search, Authorized Access.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

# I.INTRODUCTION

The fast expansion of the Internet of Things (IOT) [2, 3] has been facilitated by technical breakthroughs in wireless sensor networks [1, 2]. IOT is increasing popularity and public attention due to its instantaneity, universality, and ease of deployment, and has been widely applied in areas such as smart transportation [4, 5], healthcare [6, 7], smart homes [8, 9], and smart grids [10]. In essence, IOT is a helpful data service approach that allows users to dynamically and precisely monitor an object using real-time obtained data, which is especially beneficial in the field of healthcare [9]. As a result, creating a healthcare system employing IOT has become a new developing trend in the healthcare field. In a typical IOT-oriented healthcare system, the wearable sensor and the implanted sensor [10] collect real-time health data (such as blood pressure, heart rate, breathing rate, and others) and transfer it to the terminal device held by the designated doctor. With this method, the doctor can correctly monitor the patient's health in real-time, provide guidance on how to improve their health and a diagnosis, and be ready to deal with any potential paroxysmal diseases. Usually, the patient can choose to upload the collected health data to the cloud [11, 12], from which the patient's doctor can access it and medical institutions can use it for research. The patient would subsequently get payment for disclosing the information. The attacker, unauthorised data users, and the cloud (which is set to be semi-trusted and is interested in the stored data) would all have easy access to sensitive data privacy if we send and store the data to the cloud in the form of plaintext [13-16]. When we upload health data in encrypted form to the cloud, it is challenging for the authorized data user to separate the relevant encrypted data from the vast amount of cypher text stored there.

The issue may theoretically be resolved by enabling the data user to download and decode all of their approved access cypher text, however this is obviously impracticable due to the astronomical computational and storage costs required. Fortunately, searchable encryption (SE) was introduced as a practical and efficient solution. The data owner selects a keyword from the public keyword dictionary in a typical SE system, as seen in Fig. 1, then produces the cypher text and inserts the selected keyword. In another case, the data user first selects a search phrase from the dictionary, then creates a trapdoor tied to the search term and uploads it to the cloud.

Due to the ability to effectively retrieve cypher text, researchers have recently concentrated on SE systems for the healthcare sector [17–20]. The patient's identity should remain private even if doctors and medical institutions have permission to access it, but realistic healthcare scenarios necessitate that they be able to access a variety of patients' health data with flexibility, in accordance with the system authorization. It is surprise given that it seems like a challenging problem because attribute-based encryption (ABE) [23] totally resolves the aforementioned circumstances.

ABE provides one-to-many fine-grained access control by employing the standard of determining a data user's access authorization to determine if an attribute set conforms with an access structure. ABE schemes are further split into key-policy ABE (KP-ABE) and cypher text-policy ABE (CPABE) kinds based on their various authorization management [23]. According to the KP-ABE application scenario [24], the data user has access to a structure based on the service scope they are most interested in while the data owner is identified by a collection of descriptive attribute sets. The data is only made available to users when the access structure they choose and the attribute set of the data owner are compatible. On the other hand, in the CP-ABE application scenario, the access structure is created by the data owner themselves, and the data owner may only decode the cypher text they created if their own attribute set is included in the access

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

structure. Due to this, researchers merged ABE and SE to create attribute-based searchable encryption (ABSE), a unique cryptographic primitive that inherits the benefits of cypher text keyword search and fine-grained access control and is anticipated to be applied in the smart healthcare system [41].

However, due to the exponentiation and pairing operations' significant computing overheads in the aforementioned ABSE approaches, transmitting and retrieving health data would take longer on resource-constrained devices on the patient and doctor sides. This is obviously unacceptable in the context of quick healthcare. A few new literatures have been published to decrease the processing overheads in the online encryption phase and the decryption phase using, respectively, online/offline encryption [39] and outsourced decryption [42] technology in order to speed up encryption and decryption. Online/offline encryption, however, has no effect on how much energy or processing resources the sensor uses; it just "transfers" the operation of certain cypher text components creation to idle time. In addition, these implanted and wearable sensors regularly need to be recharged because they depend on batteries for power (some implantable sensors are even non-rechargeable, which would reduce their lifespan).

## II. LITERATURE SURVEY :

Lightweight attribute-based encryption. ABE is modelled after the fuzzily identity-based encryption (IBE) proposed by Sahai and Waters [29]. ABE, an offshoot of IBE, substitutes a set of descriptive traits for the specific identification of users. If the collection of characteristics adheres to the defined access structure, the data user could be allowed

Assembling keyword and characteristic research with encoding. The first public-key encryption with keyword search (PEKS) approach was suggested by Boneh et al. [33] in order to successfully recover keywords from the ciphertext. As a result, the literature has published various SE approaches that have enhanced access to the data without having to provide their name. One-to-many fine-grained access control and user identity privacy protection are made possible by ABE in this way. ABE is divided into two groups by authorization management: CP-ABE [23] and KP-ABE [24], each of which is suitable for a certain application scenario. The quantity of pairing and exponential operations in other ABE schemes, however, results in actual performance constraints. In other ABE schemes, the processing costs for data owners and data consumers further increase as the number of attributes increases. In response to the efficiency requirement, Hohenberger et al. [39] created the novel primitive known as online/offline ABE and created an online/offline ABE scheme based on the large-universe KP-ABE approach [25]. This technique enables the data user to quickly build the ciphertext at the cost of a few computations when the attribute set and the data to be encrypted are input by precalculating the necessary ciphertext components during the offline phase. Rao et al. [31] have presented a number of KP-ABE algorithms with compact ciphertext sizes. To generate the ciphertext, these techniques simply require a certain amount of exponential operations. The aforementioned studies, however, only focus on the data owner's computational overhead. In order to reduce the decryption overhead for the data consumer, Lai et al.'s [42] proposed the CP-ABE technique with outsourced decryption, in which the majority of the decryption activities are outsourced to a powerful semi-trusted server. The data user must do extra exponential precomputations before delivering the ciphertext to the server in order to keep the server from discovering the privacy of the data.

functionality and security [18–22]. It is astonishing how nicely ABE and SE cooperate to solve the problems of real-world ciphertext retrieval and fine-grained access control. Yu et al.'s [30] KP-ABE method leverages keyword search and doesn't add any additional steps while applying a tree access structure to instantiate a number of access

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

rules in order to lessen the user's computational load. To reduce the decryption overheads for data users, Li et al. [27] developed the ABSE approach for cloud storage with outsourced decryption. This method, however, does not account for the processing expenses spent by the data owner. To reduce the computational cost for both the data owner and the data user, Miao et al. [28] developed a lightweight finegrained searchable encryption technique with a tree access structure for fog computing. However, adding additional attributes increases the computational cost of data encryption. For the e-healthcare cloud, Wang et al. [40] proposed a CP-ABE system with keyword search that achieves policy hiddenness and considerably lowers the computational cost and storage cost for both the data owner and the data user side. A searchable CP-ABE strategy for the cloud-assisted healthcare industrial IoT was presented by Miao et al. [41]. With the online/offline technology, this technique enables the data owner to swiftly construct the ciphertext during the online encryption phase [39], but it does not really reduce the data owner's overall computing cost. Using keyword search, Cui et al. [38] developed the CP-ABE and KPABE methods, respectively. Similar to [41], it minimises the cost of building trapdoors for the data user while maintaining a high total encryption overhead for the data owner.

## III.PROBLEM STATEMENT :

Using attribute-based encryption and keyword search. The first public-key encryption with keyword search (PEKS) system was developed by Boneh et al. to efficiently retrieve keywords from encrypted text. Based on this, a variety of SE schemes with improved functionality and security have been described in the literature. It is incredible how scientists were able to combine ABE and SE to suit the requirements of fine-grained access control and encrypted text retrieval in practical applications. Yu et al. created a KP-ABE system with keyword search that uses a tree access structure to instantiate different access rules, however this approach does nothing extra to reduce the computational burden placed on the user.

In order to lower the cost of decryption for data users, Li et al. developed the ABSE cloud storage system with outsourced decryption. However, this method does not account for the processing expenses made by the data owner. To reduce the computational cost for both the data owner and the data user, Miao et al. created a lightweight, fine-grained searchable encryption solution with a tree access structure for fog computing. However, when more features are added, the computational cost of data encryption increases.

For the e-healthcare cloud, Wang et al. developed a CP-ABE technique with keyword search that achieves policy hiddenness and significantly reduces computational and storage costs for both the data owner and the data user sides. A searchable CP-ABE system for the cloud-assisted industrial IoT in healthcare was presented by Miao et al. While the data owner can swiftly generate the cypher text using online/offline technologies in this way, the overall calculation cost is not reduced. The CP-ABE and KPABE algorithms were developed by Cui et al. utilising keyword searches, respectively. Similar to this, a cunning approach minimises the cost of the data user accessing a trapdoor but the overall encryption overhead for the data owner remains significant.

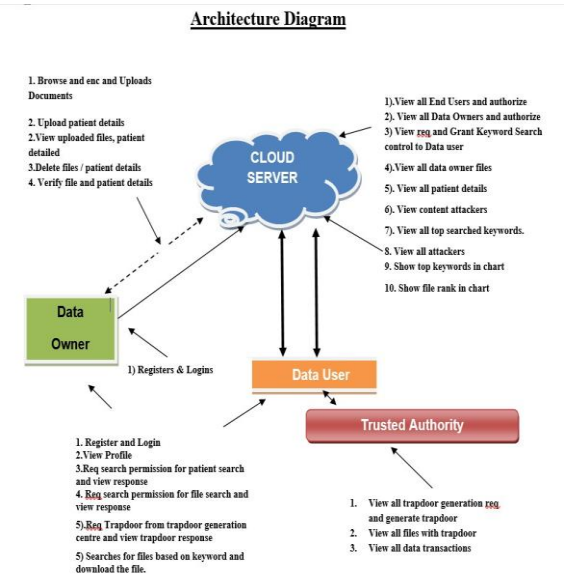
## METHODOLOGY :

We suggest the lightweight key-policy ABSE technique, which provides both fine-grained access control and cypher text search simultaneously. We design the lightweight operations of the resource-constrained devices for the patient and physician sides under realistic healthcare scenarios. We develop a workable deployment plan for our LABSE scheme under an IoT-focused and cloud-assisted healthcare system. We fully explore the security aspects in the context of healthcare and demonstrate the semantic security of the recommended LABSE scheme. The results of the

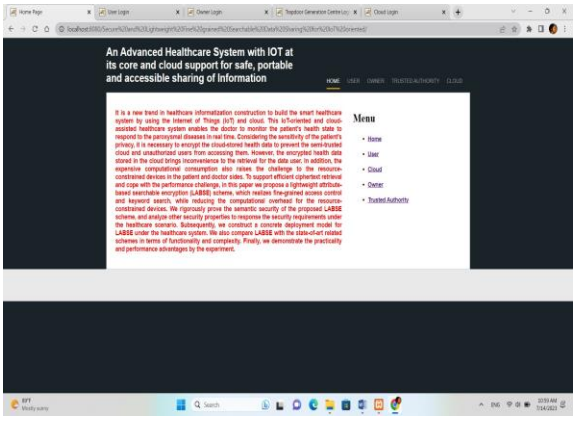
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

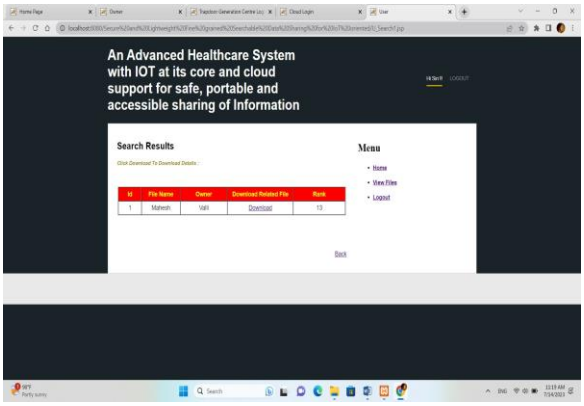
experiment demonstrate that LABSE outperforms past similar attempts in practise.

## ARCHITECTURE :




## IV. RESULTS :




## V.CONCLUSION :

The article offers the LABSE scheme and a real-world deployment methodology for a cloud-assisted healthcare system with an IOT focus. The suggested method allows keyword searching and sophisticated, light control of access, and it substantially minimizes the computational demands on devices with limited ability to process on both the patient's and the data user's sides. The semantic security of LABSE is subsequently verified and its security aspects are examined. Performance analysis shows that LABSE is useful and uses fewer resources (both computational and energy-wise) than competing approaches.

## REFERENCES:

[1] Liu Y, Fang X, Xiao M, et al. "Decentralized beam pair selection in multi-beam millimeter-wave networks, IEEE Transactions on Communications, vol. 66, no. 6, pp. 2722-2737, 2018.

[2] Chernyshev M, Baig Z, Bello O, et al. "Internet of things (iot): Research, simulators, and testbeds," IEEE Internet

of Things Journal, vol. 5, no. 3, pp. 1637-1647, 2017.

[3] Haghighi M S, Ebrahimi M, Garg S, et al. "Intelligent Trust based Public Key Management for IoT by Linking Edge Devices in a Fog Architecture," IEEE Internet of Things Journal, 2020. doi: 10.1109/JIOT.2020.3027536

[4] Feng W, Wang J, Chen Y, et al. "UAV-aided MIMO communications for 5G Internet of Things," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1731-1740, 2018.

[5] Al-Turjman F, Alturjman S. "Context-sensitive access in industrial internet of things (IIoT) healthcare applications," IEEE Transactions on Industrial Informatics, vol. 14, no. 6, pp. 2736-2744, 2018.

[6] Zhang Y, Huang X, Chen X, et al. "A Hybrid Key Agreement Scheme for Smart Homes Using the Merkle Puzzle," IEEE Internet of Things Journal, vol. 7, no. 2, pp. 1061-1071, 2019.

[7] Liao H, Zhou Z, Zhao X, et al. "Learning-Based Context-Aware Resource Allocation for Edge-Computing Empowered Industrial IoT," IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4260-4277, 2019.

[8] Al-Turjman F, Abujubbeh M. " IoT-enabled smart grid via SM: An overview," Future Generation Computer Systems, vol. 96, pp. 579-590, 2019.

[9] Natgunanathan I, Mehmood A, Xiang Y, et al. "Location privacy protection in smart health care system," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 3055-3069, 2018.

[10] Mwakwata C B, Malik H, Mahtab Alam M, et al. "Narrowband Internet of Things (NB-IoT): From physical (PHY) and media access control (MAC) layers perspectives," Sensors, vol.19, no. 11, pp. 2613, 2019.

[11] Fan Y, Lin X, Liang W, et al. "A secure privacy preserving deduplication scheme for cloud computing," Future Generation Computer Systems, vol. 101, pp. 127-135, 2019.

[12] Liu Z, Li B, Huang Y, et al. "NewMCOS: Towards a practical multi-cloud oblivious storage scheme," IEEE Transactions on Knowledge and Data Engineering, vol. 32, no. 4, pp. 714-727, 2019.

[13] Qu Y, Yu S, Zhou W, et al. "Privacy of things: Emerging challenges and opportunities in wireless Internet of Things,"

IEEE Wireless Communications, vol. 25, no. 6, pp. 91-97, 2018.

[14] Cha S C, Hsu T Y, Xiang Y, et al. "Privacy enhancing technologies in the Internet of Things: Perspectives and challenges," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2159-2187, 2018.

[15] Yang Y, Wu L, Yin G, et al. "A survey on security and privacy issues in Internet-of-

[17] Li H, Yang Y, Dai Y, et al. "Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data," IEEE Transactions on Cloud Computing, vol. 8, no. 2, pp. 484-494, 2020.

[18] Huang Q, Li H. "An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks," Information Sciences, vol. 403, pp. 2017, 403: 1-14.

[19] Behnia R, Ozmen M O, Yavuz A A. "Lattice-based public key searchable encryption from experimental perspectives," IEEE Transactions on Dependable and Secure Computing, 2018. DOI: 10.1109/TDSC.2018.2867462

[20] Liu Z, Li T, Li P, et al. "Verifiable searchable encryption with aggregate keys for data sharing system," Future Generation Things," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250-1258, 2017.

[16] Shen J, Zhou T, He D, et al. "Block design-based key agreement for group data sharing in cloud computing," IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 6, pp. 996-1010, 2019.

Computer Systems, vol. 78, pp. 778-788, 2018.

[21] Cui H, Wan Z, Deng R H, et al. "Efficient and expressive keyword search over encrypted data in cloud," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 3, pp. 409-422, 2016.

[22] Lu Y, Li J, Zhang Y. "Privacy-Preserving and Pairing-Free Multi recipient Certificate less Encryption With Keyword Search for Cloud-Assisted IIoT," IEEE Internet of Things Journal, vol. 7, no. 4, pp. 2553-2562, 2019.

[23] Bethencourt J, Sahai A, Waters B. "Ciphertext-policy attribute-based encryption," 2007 IEEE symposium on security and privacy (SP'07). IEEE, vol. 321-334, 2007.

[24] Attrapadung N, Libert B, De Panafieu E. "Expressive key policy attribute-based

encryption with constant-size ciphertexts," International Workshop on Public Key Cryptography. Springer, Berlin, Heidelberg, LNCS, vol. 6571, pp. 90-108, 2011.

[25] Rouselakis Y, Waters B. "Practical constructions and new proof methods for large universe attribute-based encryption," Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. pp. 463-474, 2013.

[26] Zheng Q, Xu S, Ateniese G. "VABKS: verifiable attribute based keyword search over outsourced encrypted data," IEEE INFOCOM 2014-IEEE Conference on Computer Communications. IEEE, pp. 522-530, 2014.

[27] Li J, Lin X, Zhang Y, et al. "KSF-OABE: Outsourced attribute-based encryption with keyword search function for cloud storage," IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 715-725, 2017.

[28] Miao Y , Ma J , Liu X , et al. "Lightweight Fine-Grained Search over Encrypted Data in Fog Computing," IEEE Transactions on Services Computing, vol. 12, no. 5, pp. 772- 785, 2019.

**ABOUT AUTHORS:**

**CH.Sri Valli Dhana Lakshmi** Currently pursuing MCA in SVKP and Dr.K.S Raju Arts & Science College(A), Penugonda affiliated to Adikavi Nannaya University, Rajamahendravaram. Her research interests include Data Structures, Web Technologies and SQL.

**B.N.Srinivasa Gupta** is working as Associate Professor in SVKP AND Dr K S Raju Arts & Science College(A), Penugonda, A.P. He received Masters Degree in Computer Applications from Andhra University and Computer Science & Engineering from Jawaharlal Nehru Technological University Kakinada (JNTUK), Kakinada, India. His research interests include Data Mining, Cyber Security, Artificial Intelligence