**AGGREGATE STATISTICS AND FINE-GRAINED CONTROL OF ACCESS FOR SECURE IOT DATA EXPORTING**

*1M. Lokesh , 2N.Kartheek ,3 K. Sravan, 4CH. Ganesh,* 5*Mr K. Chaitanya Kumar*

# *1,2,3,4bachelor Degree, Cse,* *Jayamukhi Institute Of Technological Sciences Narsampet, Warangal.*

*5Mr K. Chaitanya Kumar, Assistant Professor, bachelor Degree, Cse, Jayamukhi Institute Of Technological Sciences Narsampet, Warangal.*

**ABSTRACT:**

The need to transfer massive volumes of IoT data to the cloud has never been more pressing given the Internet of Things' (IoT) quick expansion and sharp rise in IoT devices. IoT data is often encrypted before being sent to the cloud to maintain confidentiality.

It will unavoidably make statistical analysis of them more difficult. While homomorphic encryption provides an alternate method for computing encrypted data, the IoT environment does not lend itself to its use due to its inefficiency.

How to make IoT data accessible to people with a certain set of qualities specified by data owners is another issue with encryption.

. In this research, we offer an innovative and useful IoT data outsourcing strategy based on the computation of total statistics by Corrigan-Gibbs et al. and the attribute-based cipher text policy encryption (CP-ABE). It provides the safe aggregation of outsourced IoT data as well as granular access control. Users just have to perform a little amount of processing during the upload and recovery of their data. Security study shows that our plan effectively safeguards the privacy of IoT data. Our approach performs better on both the client side and the fog server side, according to a rigorous and in-depth performance comparison.

**INTRODUCTION:**

The Internet of Things (IoT) is evolving quickly, and usage of IoT devices has expanded significantly in recent years. In 2025, there are expected to be more than 75 billion connected devices, up from more than 15 billion in 2015 [1]. Through interactions with both the real and digital worlds, these gadgets have the potential to greatly raise the living standards of their users [2].

Users of wearable technology and smart homes can, for instance, get seamless and personalised services from virtual housekeepers, physicians, and fitness instructors [3]. IoT users with constrained storage and processing capabilities have a considerable challenge in managing a continuous stream of data generated from a range of devices.

The "pay-as-you-go" cloud computing approach is a productive substitute for managing client data. A sizable quantity of IoT data may be offloaded by users to the cloud, where it can be recovered anytime necessary. However, because IoT integrates several sensor types and other devices into a range of items in our daily lives, IoT data frequently contains sensitive user data [12]. It might be user exercise data obtained from a smartwatch, the user's heart rate at a certain time obtained from the smart sphygmomanometer, or anything similar.

An obvious solution is to encrypt the data before outsourcing it in order to safeguard its security. However, there will be some brand-new issues with encryption.

How to accurately execute aggregate statistical analysis on encrypted data is the first problem. For instance, we could be interested in knowing how our health will be in the future or whether our level of exercise matches that of the average person in a certain location [10] [11].

This issue has been addressed several times.

The IoT data is encrypted by Sun et al. [12] using homomorphic encryption so that the service providers may handle user requests without obtaining the unencrypted data. However, homomorphism technology is still in its infancy. As we are all aware, the privacy homomorphism only supports a few number of homomorphism features and its encryption and decryption are highly inefficient. The broad adoption of the Internet of Things will be hampered by all these barriers. Additionally, the cloud service provider processes all of the data processing, which unavoidably results in transmission delay and worse performance when IoT device traffic to the cloud increases to remarkable levels.

The fact that the trustworthy third party is in control of homomorphism encryption and decryption, allowing it to access all the unencrypted data, is the most significant. A strong security assumption like that is quite unhelpful.

There isn't a more effective option than homomorphic encryption yet.

The second issue is how to precisely regulate access to encrypted data. The owner of the data may wish to establish an access policy and grant users who comply with it access to the relevant data. An attempt to doing this is the attribute-based encryption (ABE), which looks promising. It allows the owner of the data to specify access policies over a variety of characteristics that a user must possess in order to decode the cipher text and apply them to the data. There are two types of ABE: cipher text-policy attribute-based encryption (CP-ABE) and key-policy attribute-based encryption (KP-ABE) [7, 8]. Due to its expressiveness in specifying the cipher text access policy, the latter proves to be ideally suited for access control in the Internet of Things. In IoT data outsourcing, Huang et al. [9] establish safe data access control utilising precisely the cipher text-policy attribute-based encryption (CP-ABE). However, they failed to take into account the aggregation of this encrypted data, making data analysis difficult.

In addition, the centralised cloud computing systems will have intolerable transmission delay and deteriorated service due to the very high volume of communication between IoT devices and the cloud. Fortunately, a potential technique to address this issue is fog computing. Low latency and wide geographic dispersion are two features of fog computing, which extends the cloud computing paradigm to the network edge [5] [6]. In reality, fog computing is a tool for cloud-based services that serves as an interface between people and the cloud.

In this article, we also use fog as a support tool and provide a safe IoT data outsourcing plan. We believe that our method is the first in IoT data outsourced to achieve both encrypted data aggregation and exact access control.

**RELETED WORK :**

**AGGREGATION OF OUTSOURCED IOT DATA:**

There is an urgent need for the secure aggregation of outsourced IoT data, yet there are relatively few works that have addressed this issue. The internet of things (IoT) security and privacy problems have really caught the attention of many academics [17] [18] [19]. From the standpoint of data collection and transmission, Fan et al. [20] created safe and privacy-preserving RFID protocols to guarantee that the Internet of Things data acquired by RFID tags could only be communicated to authorised readers. the Doulas et al.

[11] suggested employing public key encryption to encrypt IoT data in order to protect data confidentiality. But as we are well aware, public key encryption has a very high computational cost, particularly in the Internet of Things, where many devices have computationally constrained capabilities. And none of the aforementioned plans take into account the collection and examination of encrypted IoT data.

Both Sun et al. [12] and Gong et al. [21] tried to use homomorphic encryption to secure data. In particular, Sun and colleagues created a trusted third party to encrypt and decode IoT data for consumers with limited resources.

IoT data can be encrypted and decrypted for users with limited resources. It implies that every piece of personal information is visible to a reliable third party. The plan devised by Gong et al. is a little bit easier, as encryption and decryption are handled entirely by the user. But they can only make a choice if the outcome falls inside the range [0,1]. Another issue with these two pieces is that the cloud server performs all data calculation, necessitating frequent communication with a large number of IoT users and giving it the potential to rapidly become the system bottleneck.

An anonymous and privacy-preserving data aggregation scheme for fog-enhanced IoT systems was recently proposed by Guan et al. [22]. They used palmier encryption to outsource the aggregation of IoT data to the cloud via fog nodes, which could achieve additive homomorphism property. However, in order to collect and aggregate data, smart devices must still perform costly computation.

**ACCESS CONTROL OF OUTSOURCED IOT DATA:**

Since IoT users may want to share their data with specific individuals, secure access control is another desirable feature in IoT data outsourcing. A well-known technology for ensuring data confidentiality and granular data access control is attribute-based cryptography. KP-ABE was used by Yu et al. [23] in the beginning of 2011 to implement fine-grained data access control in wireless sensor networks. After that, Hu et al. [24] used CP-ABE to achieve secure data communication.

between consumers of data and wearable sensors. The first framework created for lightweight IoT devices was the cloud-based, fine-grained health information access control framework proposed by Yeh et al. [25]. For Internet of Things (IoT) devices like wireless body sensors, only symmetric cryptography is necessary. However, when using ABE in fog computing directly, the computational cost in the encryption and decryption phase is linear with the complexity of policy.

When using ABE in computer fog directly, there is a complexity of policy. Fog computing was developed by Zhang et al. [26] and Huang et al. [9] to lessen the burden on IoT users. To ensure that the computation users had to perform for encryption and decryption was unrelated to the number of characteristics in the policies, they partially outsourced expensive decryption and encryption processes to the fog servers. Users still have to perform some computation, and this type of encryption will inevitably make it more difficult to aggregate and perform static analysis on data. In the context of the Internet of Things (IoT), as far as we are aware, there is no plan that allows for both limited access and encrypted data aggregation.

**FOG COMPUTING IN INTERNET OF THINGS:**

In order to reduce the burden of the cloud, as in many earlier works [4–6], we adopt fog computing as the intermediary layer between IoT users and the cloud in this paper. Low delay, geographical spread, and location awareness are some of the primary attributes of fog computing.

As a result, it can be crucial to the internet of Issues (IoT), which includes connected cars, the smart grid, healthcare, along with activity tracking purposes.

[13] suggested a distributed dataflow programming model as the foundation for IoT applications based on fog. They discussed the fundamental conditions that fog-based IoT applications needed to satisfy and noted a number of problems that had not been addressed in earlier works. The works mentioned above concentrate primarily on fog computing's fundamental ideas and importance within the context of the world wide web of things (IoT). The first mathematical formulation for fog computing was put forth by Sarkar et al. [14], who also demonstrated its importance through experimentation. They demonstrated that the mean energy expenditure in fog computing was 40.48% less than the traditional cloud computing model for a scenario where 25% of the Internet of Things applications required real-time and low-latency services.

IoT's potential use in healthcare and medicine in particular was covered by Farhan et al. [15], who also provided a comprehensive architecture of the IoT eHealth ecosystem. IoT advancements and difficulties were recently surveyed by Otway et al. [16], who also provided a number of high-yield directions that would help IoT development spread further in the fog.

**EXISTING SYSTEM:**

A general approach to protect the data confidentiality is to encrypt the data before outsourcing.

Searchable encryption schemes enable the client to store the encrypted data to the cloud and execute keyword search over ciphertext domain. So far, abundant works have been proposed under different threat models to achieve various search functionality, such as single keyword search, similarity search, multi-keyword boolean search, ranked search, multi-keyword ranked search, etc. Among them, multi-keyword ranked search achieves more and more attention for its practical applicability. Recently, some dynamic schemes have been proposed to support inserting and deleting operations on document collection. These are significant works as it is highly possible that the data owners need to update their data on the cloud server.

**PROPOSED SYSTEM:**

Suppose that there is a data user Alice, a data sender Bob, and an honest-but-curious server. When Bob wants to send some data to Alice, Bob should first obtain the pre-tag of the keyword from Alice in a secure way. Such communication channels between the senders and user are private in this phase.

Then, Bob encrypts the data, generates indexes with pre-tags and sends them together to the server. When Alice wants to search for the required encrypted data, she could generate a trapdoor with an expression and send the trapdoor to the server.

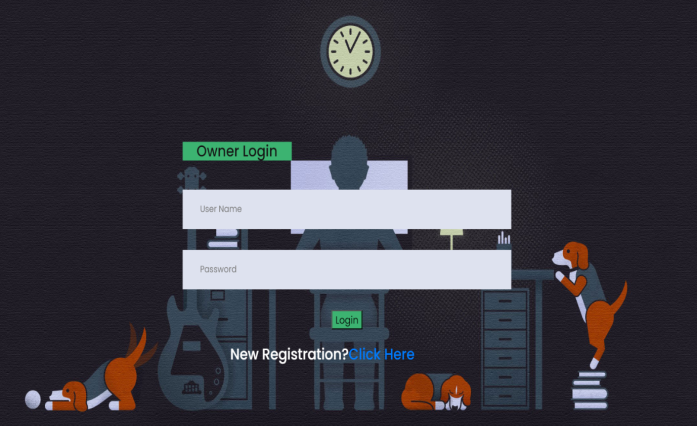
Once the server receives the search query with the index, it searches on the indexes to obtain matched encrypted data and sends them to Alice.

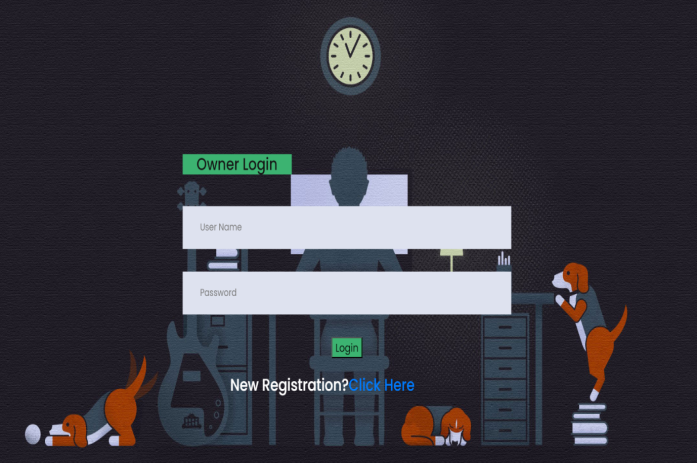
All people, including the data user and data senders, could send the encrypted data and indexes to the server, but only the user can generate the encrypted keyword.

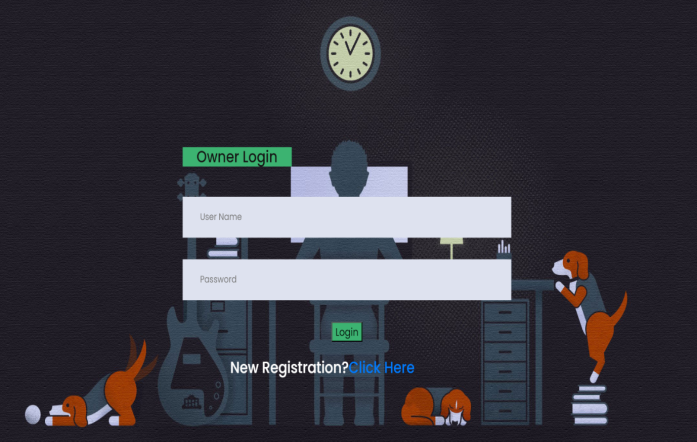
This is a multi-sender/one-user system. Note that Alice does not search with a single keyword. She could search with any n keywords of a keyword set. At the same time, the server cannot learn anything about the keywords because the proposed scheme only sends the structure of the expression tree together with the index to the server

**RESULT:**









**CONCLUTION :**

In this article, we provide a secure IoT data outsourcing strategy that can allow both real-time aggregation statistical analysis and precise control over the use of outsourced IoT data.

Fog servers can aggregate operations like addition, multiplication, and variance on IoT data provided by the data owner without knowing what data was originally provided by using Corrigan-Gibbs et al.'s calculation of aggregate statistics - Prio and Beaver's multi-party computing (MPC) protocol. We may achieve limited access thanks to cipher text-policy attribute-based encryption (CP-ABE), which only permits the user whose attributes set complies with the access policy to retrieve the associated data.

The security study demonstrates that our plan protects accuracy and data privacy. The detailed performance study and experiment show the effectiveness of our plan, proving that it is appropriate for IoT devices with limited resources like the MI phone we used in the experiment and can be used to real-time health monitoring and many other IoT scenarios. In our future work, we'll look for ways to safeguard the secrecy of results calculated by fog servers—a factor that isn't taken into account in our system. Another issue, which is also the subject of our ongoing study, is that the storage overhead in our system rises with the number of shares that a data set is divided into.

**REFERENCES:**

[1] On The Edge: Solving The Challenges Of Edge Computing In The Era Of IoT (2018), [Online]. Available: https://data-economy.com/on-the-edge

[2] G. Sun, S. Huang, W. Bao, Y. Yang, and Z. Wang, A privacy protection policy combined with privacy homomorphism in the Internet of Things[C]. International Conference on Computer Communication & Networks. IEEE, 2014.

[3] N. K. Giang, M. Blackstock, R. Lea, and V. C. M. Leung, Developing IoT applications in the Fog: A Distributed Dataflow approach[C]. IEEE 2015 5th International Conference on the Internet of Things (IOT), Seoul, South Korea, 2015: 155-162.

[4] S. Sarkar and S. Misra, Theoretical modelling of fog computing: a green computing paradigm to support IoT applications[J]. Iet Networks, 2016, 5(2): 23-29.

[5] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare[J]. Future Generation Computer Systems, 2017, 78(2): 659-676.

[6] S. M. A. Oteafy and H. S. Hassanein, IoT in the Fog: A Roadmap for Data-Centric IoT Development[J]. IEEE Communications Magazine, 2018, 56(3): 157-163.

[7] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective[J]. IEEE Internet of Things Journal, 2014, 1(4): 349-359.

[8] P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov, and A. V. Vasilakos, The Quest for Privacy in the Internet of Things[J]. IEEE Cloud Computing, 2016, 3(2): 36-45.

[9] L. Chen, S. Thombre, K. Ja¨rvinen, E. S. Lohan, A. Ale´n-Savikko, H. Leppa¨koski, M. Z. H. Bhuiyan, S. Bu-Pasha, G. N. Ferrara, S. Honkala, J. Lindqvist, L. Ruotsalainen, P. Korpisaari, and H. Kuusniemi, Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey[J]. IEEE Access, 2017, 5: 8956-8977.

[10] K. Fan, W. Jiang, H. Li, and Y. Yang, Lightweight RFID Protocol for Medical Privacy Protection in IoT[J]. IEEE Transactions on Industrial Informatics, 2018, 14(4): 1656-1665.

[11] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, A Medical Healthcare System for Privacy Protection Based on IoT[C]. 2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), Nanjing, China, 2015.

[12] Z. Guan, Y. Zhang, L. Wu, J. Wu, J. Li, Y. Ma, and J. Hu, APPA: An anonymous and privacy preserving data aggregation scheme for fogenhanced IoT[J]. Journal of Network and Computer Applications, 2019, 125: 82-92.

[13] S. Yu, K. Ren, and W. Lou, FDAC: Toward Fine-Grained Distributed Data Access Control in Wireless Sensor Networks[J]. IEEE Transactions on Parallel & Distributed Systems, 2011, 22(4): 673-686.

[14] C. Hu, H. Li, H. Yan, X. Tao, and X. Liao, Secure and Efficient Data Communication Protocol for Wireless Body Area Networks[J]. IEEE Transactions on Multi-Scale Computing Systems, 2017, 2(2):94-107.

[15] L.-Y. Yeh, P.-Y. Chiang, Y.-L. Tsai, and J.-L. Huang, Cloud-Based FineGrained Health Information Access Control Framework for LightweightIoT Devices with Dynamic Auditing andAttribute Revocation[J]. IEEE Transactions on Cloud Computing, 2018, 6(2): 532-544.

[16] P. Zhang, Z. Chen, J. K. Liu, K. Liang, and H. Liu, An efficient access control scheme with outsourcing capability and attribute update for fog computing[J]. Future Generation Computer Systems, 2018, 78(2): 753- 762.

[17] H. Corrigan-Gibbs and D. Boneh, Prio: Private, Robust, and Scalable Computation of Aggregate Statistics[C]. Proceedings of the 14th USENIX Symposium on Networked Systems Design and Implementation (NSDI’17), Boston, MA, USA, 2017.

[18] D. Beaver, Efficient Multiparty Protocols Using Circuit Randomization[C]. CRYPTO, 1991: 420-432.

[19] J. Katz and Y. Lindell, Introduction to Modern Cryptography[M]. Chapman & Hall/CRC, Cryptography and Network Security Series, 2007.

[20] PBC Library-The Pairing-Based Cryptography Library, [Online]. Available: <https://crypto.stanford.edu/pbc/>.

[31] The Java Pairing-Based Cryptography Library (JPBC), [Online]. Available: http://gas.dia.unisa.it/projects/jpbc/#.XN0OclUzaUk.