# Data Sharing with High Security on an Edge Server by Intelligent Internet of Things Users

## Pavan Kumar

### Student, GNIOT

*Abstract*: With daily technological advancements, new requirements have arisen. One of them is the internet. To push it further, they developed the Internet of Things (IOT), which is used to link smart devices to the internet. To further enhance its benefits, it is connected to the cloud, where all the data generated by it is kept, alleviating the pressure on smart devices. Edge servers are utilised in close proximity to smart devices and are capable of communication and security activities. This thesis makes an effort to reduce the time required for searching in a secure cloud on an edge server. The suggested findings extend the period of time without jeopardising security aspects. This provides a more user-friendly interface for interacting with and sharing data securely, as well as searching for and downloading it over a secure server in less time.

## Keywords: IOT, Server, Edge, Mqsql, Java

## Introduction:

The Internet of Things is the next major step of the internet, which Ashton pioneered in 1999. where real-world physical devices would be linked to the internet. This advantage enables them to be controlled from anywhere in the globe. For instance, A forgets to turn off the lights in his room before leaving for work. Someone can use IOT to turn off the lights in his workplace, saving him money, time, and energy. It may be employed in large-scale intelligent physical cyber environments. As a result, a great volume of data is generated, necessitating storage space for further analysis and processing. The Internet of Things is unable to supply vast amounts of storage capacity. As a result, we use cloud technology in conjunction with it. Cloud computing gives a large amount of storage space that is easily accessible. Apart from this, its benefit is enhanced by its on-demand accessibility and processing capabilities. When cloud is utilised in conjunction with IoT, it requires real-time data processing, minimal latency, and other capabilities that cloud cannot supply. Edge servers assist address the aforementioned shortcomings by being located adjacent to IoT devices and providing additional services such as communication, data processing, and storage activities.

These servers are semi-trusted devices, such as a mobile phone, a personal computer, or freestanding servers. They contribute to the long-range connectivity of smart devices that are used in IoT applications. They operate in close proximity to the cloud and conduct security activities. It is critical to maintain security in IOT apps since users exchange data that must be secured from malicious assault. It is beneficial to adhere to the CIA trifecta of secrecy, integrity, and availability. Only permitted users have access to the data in order to maintain confidentiality. Integrity ensures that data retains its original shape. The user is not denied access to the data when it is available.

### **Literature Review:**

Researchers are attempting to enhance the security of data exchange and search in IoT applications, however there are presently few options available. M. B. Mollah et al. proposed a lightweight cryptographic system for securing data sharing by smart devices at the edge of a cloud-based internet of things, as well as a strategy for securing data searches by authorised users at the storage level[1]. Thirumoorthy d. et al. suggested a framework for securing data while sharing and finding it using Datain cloud-based services[8]. Yi S. et al. conducted a study on the security and privacy implications of fog computing[2].

Sridevi B. addressed the problem of data security while searching for and exchanging data using the least processing cost first technique[3]. P. B. V. Rajarao et al. have developed a more secure mechanism for data exchange at the edge of the cloud-assisted internet of things[4]. Rameshwaraiah K. et al. have proposed a distribution scheme for securely sharing and searching data in Internet of Things applications[5]. Y. Tao et al. presented a mechanism for securely sharing and searching data in cloud edge collaborative storage (CECS)[6].

C. Pravallika et al. present a method for securely exchanging and searching data in IoT devices[7]. Singh J. et al. explored security concerns associated with IoT, taking into account cloud tenants, end users, and cloud providers[9]. Yi S. et al. have examined the difficulties and objectives of fog computing in conjunction with its implementation[10]. Ali M. et al. presented a functional prototype of the SeDac approach [12]. H. Kumarage et al. addressed the use of homomorphic encryption to ensure data security while searching for and exchanging data in the internet of things[13]. M. R. Palattella et al. explored 5G technologies that may be utilised for IoT[14]. J. B. Bernabe et al. have proposed a TACIoT architecture that expands the access control system and is implemented using constraint and non-constraint digital devices[15]. A. Bhagat and N. Rathee have examined numerous approaches for securely transferring data in the cloud. [16] To safeguard sensitive data from harmful assaults by attackers, security procedures must be maintained both during data exchange and search. We employed a lightweight cryptographic system to share data with others at the edge of a cloud-based Internet of Things, as well as a data searching approach to search for shared data that is kept in an encrypted form in the cloud and is accessible only to authorised users.

Along with security, we've attempted to reduce the time required for authorised users to look for data by introducing the memory module.

695

# **Proposed work:**

As part of the enhancement, this work introduced the notion of cache memory; whenever a user makes a query to the cloud server, the cloud server runs a search operation on the stored data and returns the result to the user. If a user submits the same query again, the cloud server will do the same action each time, incurring excessive compute costs and resource waste.

Maintain cache memory for all past searches to circumvent this problem. Whenever a user performs the same query, the cloud server retrieves the results from cache memory rather than doing the calculation again. FIGURE 1 illustrates a data flow diagram.



Figure 2: Screen for Cloud Storage Services

Figure 2 shows the Cloud server screen with a button to display the extension work graph. See the below screen for a search operation in figure 3.

2 Welcome aaa		×
User Screen		
Upload File Share File Search File File Encryption Time Graph	Logout	
Input		
? Enter search query		
gold silver buck		
OK Cancel		

**Figure 3: Search Query** 

In above screen of figure 6.2 I gave the query as 'gold silver truck', and this query is not available in cache, so the cloud server will perform entire search computation and send the result back to user.

📓 View Search Result		
Username	Filename	
aaa	al.txt	
aaa	a2.txt	
aaa	a3.txt	
Download File		

# **Figure 4: Search Results**

Above the screen, it is showing the search result in figure 4.

Cloud Storage Services Started	
SECURE DATA SHARING AND SEARCHING AT THE EDGE OF CLOUD-ASSISTED INTERNET OF THINGS	
Cloud Storage Screen	
Client Request Processing Status	
Cloud Storage Services Started	
Search result sent to user for query 229sZA,c21sdmWy,dWJYZs- Search result not found in cache	
Extension Comparison Graph Hormal Search Time Ve Cache Search Time	
Figure 5: Search Results	

In the above screen, figure 5 at the cloud side showing status as search not found in cache If I execute the same query again, then Cloud will obtain the result from cache seen in figure 6.

	🛃 Welcome aaa		🛛	<b>i</b> 8 X
	Input	×		
	Upload File S	Enter search query	Graph Logout	
		gold silver truck		
		OK Cancel		
			•	

## Figure 6: Search Again with Cache

Below is a search screen for the result with cache memory saving in figure 7.

📓 View Search Result		
Username	Filename	
aaa	al.txt	
aaa	a2.txt	
aaa	a3.txt	
Download File		

Figure 7: Results for search from Cache

### **Results:**

The primary result parameter is the edge server's search time. This was accomplished by incorporating cache memory into the edge server. It will establish a memory for previously saved material and increase the speed with which the searched phrases are processed. It is very advantageous when a large text file is uploaded to the server. The other outcome parameter is security, which is accomplished in the early work through a key agreement procedure and hash method. The graph in Figure 9 illustrates the improvement over the previous strategy. On the cloud side, the search status is shown in the figure 8 below.

🖪 Cloud Storage Services Started	
SECURE DATA SHARING AND SEARCHING AT THE EDGE OF CLOUD-ASSISTED	
INTERNET OF THINGS	
Cloud Storage Screen	
Client Request Processing Status	
Cloud Storage Services Started	
Search result sent to user for query 229s2A==,c2lsdmWy,dWJ1Y2s= Search result not found in cache	
Search result sent to user for guery 12952A+=,c2lsdmWy,d0471Y2s= from cache memory	
Extension Comparison Graph	
Hozmal Search Time Vs Cache Search Time	

Figure 8: Result in Cloud Server for search from Cache

By clicking on the 'Extension Comparison Graph' button, one can see execution time for both cloud complete search and cache search in the visual graph in figure 9.



Figure 6.8: Result Graph for Faster Speed

In above graph shows that normal search took from execution time compared to cache search.

## **Conclusion:**

This paper proposed a lightweight cryptographic and speedier framework for IoT-enabled handsets to exchange data at the pinnacle of cloud-assisted IoT. All security-related tasks are delegated to a network of exhausting outskirt PCs. This thesis examines the criteria outlined above in relation to current choices for asset-restricted intelligent devices. A data search framework for locating and sharing relevant data by authorised buyers in databases where all data is encoded, despite early concerns about information sharing security. Additionally, the security and speed of execution investigations demonstrate that the proposal is realistic and reduces the costs of all companies in our framework for counting and communication. The whole system is safe, quicker, and encrypted successfully in all cloud storage formats.

## References

[1] SivannarayanaNerella, G.Sateesh "Confederate Process Key Agreement Scheme For Cloud Assisted Vehicular Internet Of Things" International Journal of Research in Advent Technology, Special Issue, March 2019 E-ISSN: 2321-9637.

[2] C. Pravallika, P. Sukanya "Secure Data Sharing and Searching at the Edge of CloudAssisted Internet of Things" International Journals of Advanced Research in Computer Science and Software Engineering ISSN: 2277-128X (Volume-8, Issue-4),2019.

[3]Hind Bangui , Said Rakrak, Said Raghay and BarboraBuhnova "Moving to the Edge-Cloud-of-Things: Recent Advances and Future Research Directions" Electronics 2019, 7, 309

[4]L. Minh Dang , Md. JalilPiran, Dongil Han, Kyungbok Min and Hyeonjoon Moon "A Survey on Internet of Things and Cloud Computing for Healthcare" Electronics 2019, 8, 768.

[5]Sampath Kumar Y R and Champa H N "An Extensive Review on Sensing as a Service Paradigm in IoT: Architecture, Research Challenges, Lessons Learned and Future Directions"International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 6 (2019) pp. 1220-1243.

[6]Sukhpal Singh Gilla, Peter GaDr.K. Praveen Kumarrraghan, RajkumarBuyy "Fog enabled cloud based intelligent resource management approach for smart home IoT devices" Institute of Electrical and Electronics Engineers 2019.

[7] FaguiLiu ,Zhenxi Huang and Liangming Wang "Energy-Efficient Collaborative Task Computation Offloading in Cloud-Assisted Edge Computing for IoT Sensors" Received: 22 January 2019; Accepted: 26 February 2019; Published: 4 March 2019.

[8] ShreshthTulia,b, RedowanMahmuda, , ShikharTuli c, RajkumarBuyya "FogBus: A Blockchain-based Lightweight Framework for Edge and Fog Computing" International Research Journal of Engineering and Technology (IRJET), Received 2 October 2018 Revised 13 March 2019 Accepted 12 April 2019 Available online 13 April 2019.

[9]FanBi, SebastianStein et al.,"A Truthful Online Mechanism for Allocating Fog Computing Resources"AAMAS 2019, May 13-17, 2019, Montréal, Canad.

[10]Igor Leão dos SantosA, Flávia C. DelicatoB, Paulo F. Pires B, Marcelo PitangaAlvesC, Ana OliveiraD, Tiago SalvianoCalmonD "Data-Centric Resource Management in Edge-Cloud Systems for the IoT "Open Journal of Internet Of Things (OJIOT) Volume 5, Issue 1, 2019 ISSN 2364-7108.

[11]Arun K Mani, Shreevani D, Samra said, M.Gokilavani, Unnikrishnan K N "A Review: Iot And Cloud Computing For Future Internet "International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056, Volume: 06 Issue: 05 | May 2019.

[12] SabeenJavaid, HammadAfzal, Muhammad Babar, FahimArif, "An Attack-Resilient Cloud-Assisted IoT System" Institute of Electrical and Electronics Engineers, 10.1109/ACCESS.2019.2897095, IEEE Access.

[13] P. Har i Naveen, K. Viswaprasad "Secure Data Sharing and Searching at The Edge of Cloud-Assisted Internet of Things" International Standard Serial Number (ISSN) DECEMBER/2018

[14] A.V.Soujanya, Budur Naveen Kumar Reddy, Shruthi.P, Sushmitha.P.T, Dr. Aradhana.D "Reliable Data Sharing And Searching At The Edge Of Cloud With The Help Internet Of Things" International Journal Of Professional Engineering Studies, Volume 10 /Issue 1 / MAY 2018.

[15] SnehaSureddy, K. Rashmi, R. Gayathri and Archana S. Nadhan "Flexible Deep Learning in Edge Computing for IoT" International Journal of Pure and Applied MathematicVolume 119 No. 10 2018, 531-543.

[16] AbhishekJaiswal ,Mohit Kumar Nayak "Reducing the Computation and Communication Overhead of IoT Smart Devices through a Lightweight Cryptographic Scheme" International Standard Serial Number (ISSN) Volume 7, Issue XI, November/2018.