RELIABLE DATA SHARING AND SEARCHING AT THE EDGE OF CLOUD WITH THE HELP INTERNET OF THINGS

[1] A.V.Soujanya, [2]Budur Naveen Kumar Reddy,[3]Shruthi.P,[4] Sushmitha.P.T,[5]Dr.Aradhana.D

[1,2,3,4]B.E Student, Department of CSE, Ballari Institute of technology and management, Ballari District, Karnataka, India, 583104.

[5]Associate Professor, Department of CSE, Ballari Institute of technology and management, Ballari District, Karnataka, India, 583104

Abstract:-

Over the last few years, smart devices can able to communicate with each other and with Internet/cloud from short to long range. As an outcome, a new paradigm is introduced called Internet of Things (IoT). Be that as it may, by using cloud computing, asset restricted IoT savvy smart devices can get different advantages like offload data storage and preparing trouble at cloud. To help inactivity latency sensitivities, constant information handling, versatility and high information rate IoT applications, working at the edge of the system offers a more advantages than cloud. In this paper, we propose an effective information sharing plan that enables savvy smart devices to secure shearing schema to others at the edge of cloud-assisted IoT. Furthermore, we likewise propose a secure searching scheme to search client query own/shared information on capacity. we analyse, we dissect the execution in view of handling time of our proposed scheme. The outcomes exhibit that our plan can possibly be viably utilized as a part of IoT applications.

INTRODUCTION:

The Internet of Things (IoT) is considered as a future internet that extends the connection of the internet to all kinds of real-world physical smart devices. By autonomous cyber-physical environments in the area of smart grids, smart cities, smart homes, smart medical and healthcare systems, wearable technologies, transportation systems, etc. However, the majority of these devices are part of a large platform, hence, a huge amount of data are generatedthat requires high computational capabilities for storage, processing, and analyzing purposes in a secure and efficient manner. On the other hand, cloud resources have virtually unlimited storage and processing capabilities with scalability and on-demand accessibility anywhere. Thus with the help of the cloud, the IoT smart devices can relieve the burden of limited resources. For IoT applications, smart devices require low latency, high data rate, fast data access, and real-time data analytics/processing with decision-making and mobility support. Due to several drawbacks, the cloud cannot fulfill the aforesaid requirements. These edge servers are any personal device or mobile device, stand-alone servers, or network devices that are hosted within one hop far from the end devices. a secure data-searching technique is needed to search and retrieve the shared

data by authorized devices. At present, there are few solutions to address the challenges of secure data sharing and searching in clouds. Typically, to ensure confidentiality of shared data, symmetric key, public key, and homomorphic encryption-based mechanism are currently used. Access control policies based on access control list and dynamic attribute are used for access control purposes. Searchable encryption based on symmetric and public keys are used for searching the desired data. In all these schemes, for data security, major security-oriented processing such as encryption, decryption, and access control mechanisms are handled by the user's device itself.

2. RELATED WORK

The IoT paradigm holds the promise to revolutionize the way we live and work by means of a wealth of new services, based on seamless interactions between large amounts of heterogeneous devices. After decades of conceptual inception of the IoT, in recent years a large variety of communication technologies has gradually emerged, reflecting a large diversity of application domains and of communication requirements. Such heterogeneity and fragmentation of the connectivity landscape is currently hampering the full realization of the IoT vision, by posing several complex integration challenges.

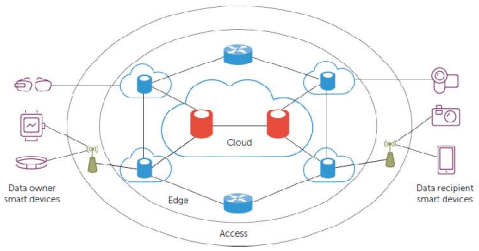
Internet of Things typically involves a significant number of smart sensors sensing information from the environment and sharing it to a cloud service for processing. Various architectural abstractions, such as Fog and Edge computing, have been proposed to localize some of the processing near the sensors and away from the central cloud servers. In this paper, we propose Edge-Fog Cloud which distributes task processing on the participating cloud resources in the network. In this paper, we proposed the Edge-Fog cloud, a decentralized cloud model for handling computation-based, high volume and distributable data such as that generated by IoT. The model builds on the existing Edge and Fog cloud approaches and provides data resilience through a centralized data store.

The vision of the Internet of Things is to allow currently unconnected physical objects to be connected to the internet. There will be an extremely large number of internet connected devices that will be much more than the number of human being in the world all producing data. These data will be collected and delivered to the cloud for processing, especially with a view of finding meaningful information to then take action. However, ideally the data needs to be analyzed locally to increase privacy, give quick responses to people and to reduce use of network and storage resources.

Internet of Things (IoT) brings more than an explosive proliferation of endpoints. It is disruptive in several ways. In this chapter we examine those disruptions, and propose a hierarchical distributed architecture that extends from the edge of the network to the core nicknamed Fog Computing. In particular, we pay attention to a new dimension that IoT adds to Big Data and Analytics: a massively distributed number of sources at the edge.

3. FRAMEWORK

Proposed Framework Overview:-



In this paper, by considering the aforementioned limitations of current solutions for resource-limited smart devices, we propose a lightweight cryptographic scheme so that IoT smart devices can share data with others at the edge of cloud-assisted IoT wherein all security-oriented operations are offloaded to nearby edge servers. Furthermore, although initially we focus on data-sharing security, we also propose a data-searching scheme to search desired data/shared data by authorized users on storage where all data are in encrypted form.

First, we propose a secure data-sharing scheme at the edge of cloud connected IoT smart devices that utilizes both secret key encryption and public key encryption. In this scheme, all security operations are offloaded to nearby edge servers, thereby, greatly reducing the processing burden of smart devices.

Next, we propose a searching scheme to search desired data securely by authorized users within encrypted, stored, shared data in edge/cloud without leaking keyword, secret key, and data, thereby reducing both computation and communication overhead during search and data retrieval.

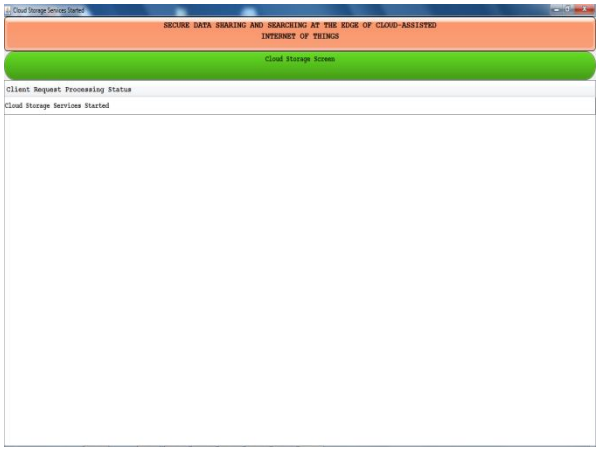
Then, we show the verification process of the shared data as well as data retrieval after searching. Hence, our proposed scheme attains the integrity of shared data and searching resultant data.

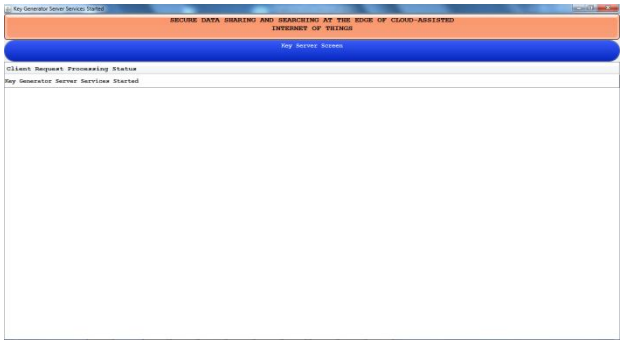
Finally, we analyze the performance of our proposed scheme and prove that our scheme is efficient and can be used in IoT applications.

4. EXPERIMENTAL RESULTS

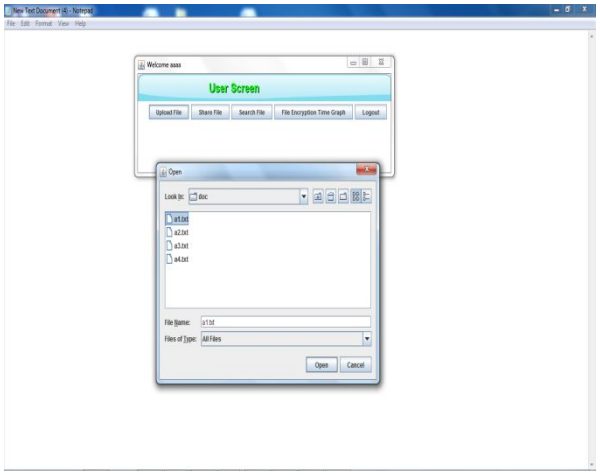
In this experiment, we used three servers which are included in our proposed scheme and those include the servers to store the data. We have the key generator server it will provide the keys for security and provide the security for user data .In edge server it provide the security for the public and private keys to perform the operation regarding to the user data.

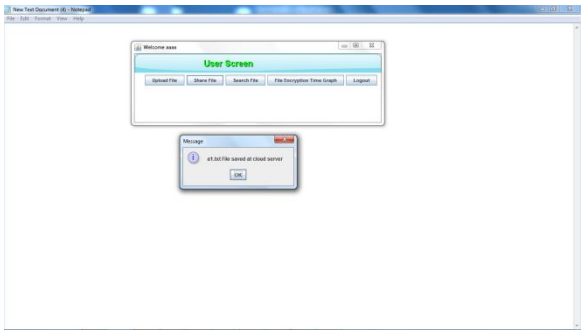
The edge servers are semitrusted and secure entities located at the proximity of smart devices that are capable of sharing data with a number of smart devices. It is responsible for security-oriented operations such as secret key generation and management, encryption, and decryption. The edge servers are maintained by clouds. Moreover, the edge servers provide data storage and processing of the smart devices.





When you are uploading the data in the cloud we can perform the operation called upload we can upload the user data with encryption into the cloud. If we need to share the data we need to give the access permission to the person in search the file when you search the query the that will provide proper information regarding to the user query.





5.CONCLUSION

In this paper, we present a proposed data-sharing and -searching scheme to share and search data securely by IoT smart devices at the edge of cloud-assisted IoT. The performance analysis demonstrates that our scheme can achieve better efficiency in terms of processing time compared with existing cloud-based systems. In future work, we plan on authenticating and accessing control challenges in this area. We hope that our proposed scheme is practical to be deployed and opens a new door in edge-oriented security research for cloud assisted IoT applications.

Reference:-

1. M.R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, et al., “Internet of Things in the 5G Era: Enablers, Architecture, and Business Models,” IEEE J. Selected Areas in Communications, vol. 34, no. 3, 2016, pp. 510–527.

2. L. Wang and R. Ranjan, “Processing Distributed Internet of Things Data in Clouds,” IEEE Cloud Computing, vol. 2, no. 1, 2015, pp. 76–80.

3. M. Satyanarayanan, P. Simoens, Y. Xiao, P. Pillai, Z. Chen, K. Ha, et al., “Edge Analytics in the Internet of Things,” IEEE Pervasive Computing, vol. 14, 2015, pp. 24–31.

4. S. Yi, Z. Hao, Z. Qin, and Q. Li, “Fog Computing: Platform and Applications,” 2015 3rd IEEE Workshop Hot Topics Web Systems and Technologies (HotWeb), 2015, pp. 73–78.

5. J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, “Twenty Security Considerations for CloudSupported Internet of Things,” IEEE Internet of Things J., vol. 3, no. 3, 2016, pp. 269–284.

6. M. Ali, R. Dhamotharan, E. Khan, S. U. Khan, A.V. Vasilakos, K. Li, et al., “SeDaSC: Secure Data Sharing in Clouds,” IEEE Systems J., vol. 99, 2015, pp. 1–10.