An Integrated Architecture For Iot Based Data Storage In Secure Smart Monitoring Environment

Mr. Sunil Raj Y, Dr. Albert Rabara S

Abstract— IoT is seen to be daughter of internet, placing its foot and making revolution in every area of day to day life. Cloud a revolutionary technology gives hand to IoT, so that data generated by devices can be stored and processed with the help of data stores. Labor of IoT in healthcare turns its name as smart healthcare. Smart monitoring in health is a typical task and this paper presents an integrated secure architecture for smart monitoring system. Along with existing prototype including security may help providing integrity to data in the storage to a greater extent.

Index Terms— Internet of Things (IoT), Data Storage Security, Cloud Storage, Object Storage, Data Integrity.

1 INTRODUCTION

Internet of Things is found as sacred sign for healthcare industry among other major area of concerns. IoT known as a world-wide physical connection of things, connected and can be controlled distantly. To a greater extent devices are well-found using intelligent sensors, connecting things suits at ease [1].

Data collected over innumerable devices can be stored in virtual storage, which is said organized using technology called cloud. Since volume of data collected over network of device is huge, data storage would be a better storage option.

Cloud having a distributed sense for handling distinct services for users distributed in different geographical locations. As data centre cloud implements a demilitarized zone, where largely sensitive information is stored.

Being largest storage existence of duplication makes servers an untrusted entity. Lack of control, multi–tenancy concepts and virtualization devour high security threats connected to information stored in traditional data centre [4].

As data stored is on several third-party servers, [4] issues user have to face while using cloud storage services are deployment of storage, virtualization and availability of storage, data organization, migration, load balancing, deduplication of data and security.

Since provider's holds full control, which lets performing tasks with data/file like copying, destroying, modifying and so on. Various security concerns are involved in storage, where major issues are [5] privacy, integrity, recoverability and vulnerability, improper media sanitation, backup, outage.

Chief chore is providing healthier service to data storage user or customer always. Though user friendliness is important factor, providing better service which includes security and integrity is essential. Hence to increase the efficiency of system a good security mechanism is very essential.

Consequently in-order to provide protection to data stored on cloud data centers, protecting data by preserving integrity should be a major tasks.

Fig. 1.1 Simple Structure of Data Flow in Cloud Storage

As data collected using sensor devices, can be stored on cloud and be used for processing, while processor may be on cloud or not. The present security mechanisms found to be providing security measures yet integrity requires serious concern. The proposed work provides more integrity by integrating mechanism for recovery and third party auditing.

The paper is organized as follows: Section II provides a review of motivation, Section III presents the architecture for enhancing the security concerns, Section IV presents the theoretical analysis of the proposed architecture, Section V presents conclusion of the paper.

2 LITERATURE REVIEW

[2] IoT a global network infrastructure where physical/ virtual 'Things' have physical attributes, identities, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into information network.

IoT composed of many connected devices depending on sensors, communication, networking, and information processing technologies [3].

Security is substantial concern that limits global users from espousing cloud technology. The noteworthy issues are Integrity where system preserves a suitable depiction of intended data which was not modified by an authorized person and Availability which sureties the readiness of data access [12].

[6] Twin MDS code is robust against passive eavesdropper and data repair process of failed node. The output derived using regenerating codes framework gives better results than MSR and MBR codes.

[7] Here the need of object storage system for massive unstructured digital static data and its relevant architecture is

- *Dr. S. Albert Rabara is working as Associate Professor in the Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamilnadu, India. He has 21 years of experience in teaching and 13 years of experience in research. E-mail: a_rabara@yahoo.com*
- *Mr. Y. Sunil Raj is currently working as Assistant Professor in the Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamilnadu, India., E-mail: ysrsjccs@gmail.com*

the major concern. Object storage in cloud suits better for unstructured static data, which is also used for most modern archived storage. Advantage of this storage is its scalability, Meta data management, flexibility and security.

[8] Proposes pipelined cloud-of-clouds storage approach, which speed up the dispersal algorithms, calculation operations executed with transmission operations in parallel while depending on different resource in nature. With this notion, we design a pipeline-based architecture to speed up the dispersal algorithms in the cloud-of-clouds storage paradigm.

[9] The work introduces, private cloud infrastructure based design, for providing security in access and sharing of files and easy maintenance. It adds time efficient storage and sharing of files while nod disturbing easiness and security. For better functionality compression methods can be introduced. Design best suits in situations like fairly unused storage centers over which a cloud is built.

For making up a secure and reliable system [10], proposes a twin code framework which is most suitable for distributed storage, by which it may efficiently handle data reconstruction and efficient node repair.

To secure the cloud storage [11], introduces biometric based framework. Techniques such as chaotic maps, key generation and reed-solomon decoding are used in various levels of security aspects.

3 Integrity in Data Storage

Essential components like accuracy, consistency, fidelity and validity of remotely stored data are called data integrity. Main concerns on integrity, is that data is retrievable without any loss or corruption issues. As it is available anywhere anytime this is to be addressed.

Integrity can be corrupted by various errors such as malicious attacks, S/W bugs, H/W malfunctions or human errors. Therefore availability and correctness of data turn into a most important demand for customers. Solution to challenge of data integrity would be made by, checking and auditing [12].

Cloud Storage Services is in need to convince that data has remained unaltered and it is kept safe from corruption, modification or unauthorized disclosure. Based on this the work proposes an architecture in the following section.

4 Proposed Architecture

An intelligent smart monitoring system is introduced here, where the work is not only concerned about smart monitoring but also largely concerned about adding security to data storage. The purpose is designated in fig 3.1.

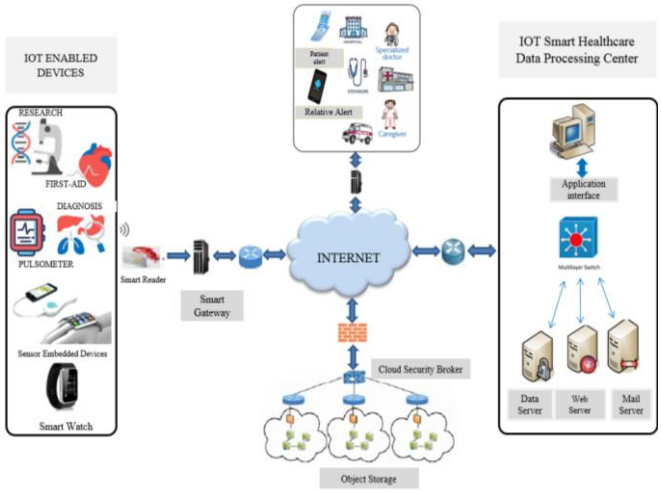

Fig. 3.1. Security Architecture- Public Cloud Storage

The proposed architecture fig. 3.1., discloses five different components, starting with smart monitoring unit where sensors involve a lot and next is data processing center, the third is alert module and the major part concerned is cloud storage also called as data storage. The security mechanism proposed maintains the integrity and security of the data on the data storage.

With respect to access of data storage methodology followed is to keep data secure while maintaining its integrity as in fig 3.2. Along with usual authentication and authorization third-party audit mechanism is being introduced [11]. By this security properties can be monitored by which the integrity of data is assured.

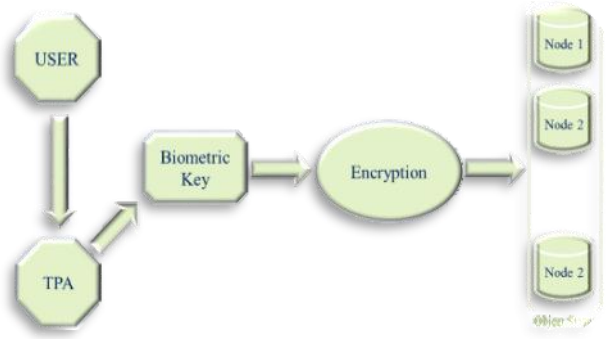

Fig. 3.2. Security Mechanism to Maintain Integrity

In order to provide security to the distributed storage, [10] framework is drawn focusing on node failure. An encoding technique used splits message into fragments and is represented through matrix for encoding. The recovery mechanism improves the security of data at the time of passive attack. As the node fails, the Type 2 nodes are referred, which return a combination of data. From this result the actual data can be recovered using the identity matrix. This uses MDS erasure technique for encoding and decoding data.

Apart from security provided, data can be infected during the file synchronization since it was stored in a distributed way. Addressing this [11] has evaluated a security

framework which is based on biometric data. The authentication is based on secure sketch technique. This allows generation of cryptographic key. Chaotic map are involved in key generation. Key generation process is divided in to two sub-processes, a key-generation referring the cipher key K and a secure sketch returning a public output S.

Fig. 3.2, explains that in order to maintain secrecy the captured fingerprint is not sent to the cloud provider. The data is send if the secure sketch and the enrolled finger print data match. The decoding technique used is one same as that is used in Twin-MDS framework.

It is clear that security can be provided in better way to secure the privacy of the data. Better solution towards problem occurring to the data at rest addressed, where the security properties are being monitored with the help of Third Party Audit [11].

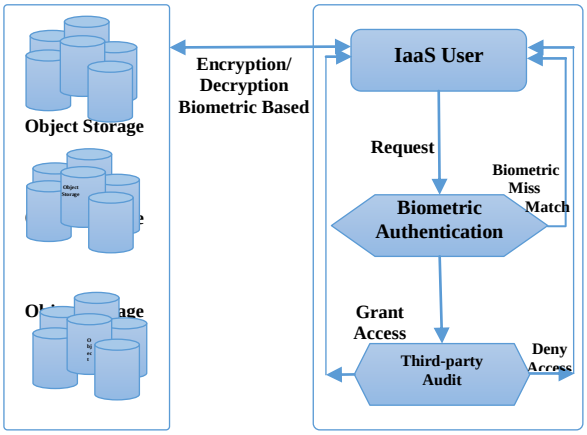

Fig. 3.2. Mechanism to Authorize User Access

Protocols will be drawn in such a way that customer could define permission for files that are in use. Access Control List is used to specify the user access permission. The Cloud Broker is one of the components in this framework, who stores the metadata of each file to enable authorized users based on the read / write permission defined in ACL. Use of transaction Log is another important fact that avoids violation of security properties. For each and every request from the user for a file, a validation process is carried out by TPA referring the Credentials of Cloud Broker and Cloud Provider. Twin code model [9] is used to add reliability to the data as data is stored on a distributed fashion. Added to this is the biometric based key generation technique as it will be helpful in encrypting the data that will be only available for the intended user and intruders are now at the risk of unavailable key for decryption. In-order to decode the data read-solomon decoding mechanism is to be adopted [10]. These mechanisms will very well provide a better security to the data and the storage, thereby assuring the integrity of the data to a greater extent.

5 RESULTS AND DISCUSSION

Data received from multiple sensor nodes strewn over cloud object storage. This process actually includes twin code framework, where passive attacks are avoided.

In-order to overcome risk of active attacks by intruders, third-party audit is included along with biometric based key generation. This provides better integrity, as TPA adds an activity log. The users accessing storage can be monitored and thereby integrity of data is preserved.

Data at rest may happen to be destroyed due to node failure, which can be minimized by implementing recovery mechanism, based on twin code model. Twin code framework [9] performs well during node failure which provides security to both DSS and data that are transmitted. It is understood that security of data here is very much secure. Assuming nodes used would be X and this depends on size of the file that is send by user. Scattering of data is done in such a way that y size of data will be strewn to X nodes.

Proposed mechanism increases safety during passive attack, as square matrix is used to keep track of data that is intended to be used for recovery. As node fails, Type 2 nodes are referred, which return a combination of data. From result which is generated, actual data could be recovered using matrix. Here MDS erasure method best suits for encoding and decoding data.

Access Control List specify access permissions, where cloud broker stores metadata of file to enable authorized users read/ write permission. Use of transaction Log is used to keep track of each and every transactions. This not only helps keep track of transactions, also avoids violations of security properties. Validation is mandatory for access of file which is carried out by TPA referring the Credentials of Cloud Broker and Cloud Provider.

6 CONCLUSION

The study discloses that proposed architecture is better in handling data at rest. Also preserves data from intruders to a greater extend in-order to keep up integrity. Integrity of data is well-looked-after in healthier manner. As security properties are checked, confidentiality is higher in such a way that it can be used for high level processing such as medical applications, military applications where sensitive data is involved.

In future study will be extended towards elaborating on various security concerns introduced in proposed architecture.

References

[1] Y. Wu, Q. Z. Sheng, S. Zeadally, "RFID: Opportunities and challenges," in Next-Generation Wireless Technologies, N. Chilamkurti, Ed. New York, NY, USA: Springer, 2013, pp. 105–129.

[2] R. van Kranenburg, "The Internet of Things: A Critique of Ambient Technology and the All-Seeing Network of RFID", Amsterdam, The Netherlands: Institute of Network Cultures, 2007.

[3] L. Tan, N. Wang, "Future internet: The internet of things," in Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE), Chengdu, China, 2010, pp. 376–380.

[4] Joel J. P. C., Dante B. R., Heres A., Murilo H., Rafael M., Jalal Al-Muhtadi, Victor Hugo C., "Enabling Technologies for the Internet of Health Things", IEEE, 2018, ISSN: 2169-3536.

[5] Samhita Kanthavar, "Design of an Architecture for Cloud Storage to Provide Infrastructure as a Service (IaaS)", IEEE, 2017.
[6] Samundiswary.S, Nilma M Dongre, "Object, Storage Architecture in Cloud for Unstructured Data", International Conference on Inventive Systems and Control, IEEE, 2017.
[7] Saswati, Anirban, "A Parallel Technique for Storage Defragmentation in Cloud", 2016 Second International Conference on Research on Computational Intelligence and Communication Networks, IEEE, 2016.
[8] Jiajie, Jiazhen, Yangfan, Xin, "Cloud-of-clouds Storage Made Efficient: A Pipeline-based Approach", IEEE International Conference on Web Services, 2016, pp724–727.
[9] Marina, Velkaska, Paunkoska, "Efficient distribution and improved security for reliable cloud storage system", IEEE EUROCON 2017–17th International Conference on Smart Technologies, 2017, pp727 – 732.
[10] Nakouri, Hamdi, Kim, "A New Biometic Based Security Framework For Cloud Storage", 13th International Wireless Communication and Mobile Computing Conference, 2017, pp390 – 395.
[11] Carvalho, Castro, Andrade, "Secure Cloud Storage Service for detection of security violations", 17th IEEE/ ACM International Symposium on cluster, cloud and grid computing, 2017, pp715 – 718.
[12] Raut, Itkar, "A Survey On Data Integrity Of Cloud Storage In Cloud Computing", International Journal of Advance Foundation and Research in Computer, 2014.