Enhancing the Data and Storage Security for Integrated Cloud and IoT System Using Secure Hash Algorithm

[1]Ayesha Siddiqha Mukthar, [2]Dr. Jitendra Sheetlani
[1]Research Scholar, Sri Satya Sai University of Technology and Medical Sciences, Sehore
[2]Associate Professor, Sri Satya Sai University of Technology and Medical Sciences, Sehore

Abstract

With the rapid growth in cloud users and they store number of data in cloud, security of cloud becomes most essential. Whereas cloud offers the facility to users that they can access the data from anywhere and anytime. Cloud computing provides consistent and irrepressible infrastructure for users to remotely store data and use on-demand applications and services. Conversely, the outsourced data is not every time reliable because of the loss of physical control and possession over the data. Internet of things is one of the most emerging and popular technology, which has changed our life, by impacting different areas such as shopping, enterprise production, storage, monitoring physical devices, etc. An enterprise has to store data generated from the Internet of Things and this data grows exponentially, it forces to think about cloud storage for storing IoT data. Here the proposed system uses the secure hash algorithm for enhancing the security of Cloud based IoT system.

Keywords: *Cloud Users, Auditing, Cloud Computing, Secure Hash Algorithm, Data center, Reliability, Integrity.*

Introduction:

The IoT can be considered as one type of environment in which all physical objects, peoples and animals are having unique identity and they are able to transfer data over the network without any interaction1. IoT is the combination of different technologies, it evolved the internet, wireless technologies and micro-electromechanical systems (MEMS) [1]. This terminology can be considered as the Internet of Everything. A thing presents in the IoT environment can be a man-made object, a person with a heart monitor implant, any animal with a biochip transponder and any vehicle with sensor. All these things are assigned with one unique IP address and has the ability to transfer data over the Internet. So far, IoT closely related to Machine-to-Machine (M2M) communication in manufacturing, oil, gas and power industries. The IPv6s having huge address space and with help of IPv6 we can assign a unique address to each object present on the surface of earth. IPv6 is a very significant feature for the development of Internet Things. The Internet of Things (IoT) hypothesis is that the objects or things interact and exchange large scale information. Now days, organizations use IoT devices to collect real time and continuous data and make better business decisions to increase customer satisfaction. An enterprise has to store data generated from the Internet of Things and this data grows exponentially, it forces to think about cloud storage for storing IoT data. The cloud appears to be a noticeable choice for IoT data storage, various organizations store this information on site considering it is either costly or sensitive to store on the cloud [2]. The cloud has more advantages to store IoT data than on-premises storage. First, a direct connection is provided between the devices and the public cloud provider. This direct link allows to store data faster therefore, it need less storage and lower per-device cost. Second, data management and storage management is the cloud provider problem therefore organization has to use the service only. Cloud becomes an ideal storage location for storing and processing IoT data but there are some problems to use the cloud for IoT data Storage. The main and major issue is security [4] of cloud storage. In many situation data collected from IoT devices is more sensitive or very important for the organization. When cloud storage is used, then organizations worried about the cloud security issues [3]. This paper uses the SHA (secure hash algorithm) for making the integrated cloud based IoT system secure.

2. Security Threats facing IOT and Cloud Computing

In these sections, major security threats of IoT and Cloud computing are explored. They include data threats, network threats, cloud environment threats, physical attack, unauthorized access to RFID, and sensor nodes security threats [5,12].

Data Threats

While transmitting data it is always important to hide from observing devices on the internet. Data is a valuable resource to any organization and person, and the rate of shifting data to the cloud is increasing every day. The biggest challenge in achieving cloud-computing security is to secure data, this is because clients depend on the service providers to ensure that the data is secure. The properties of data security maintained by the cloud include confidentiality, integrity, authorization, data availability, and privacy. Improper handling of data by the cloud may lead to data threats, which include data breach, data loss, integrity violations, and unauthorized access.

Data Breach

It involves leakage of user or organization data to an unauthorized user. This may happen due to malicious attackers who access the system in an unauthorized way. It can also happen accidentally due to infrastructure flaws, operational issues, and insufficiency of authentication or audit controls.

Data Loss

It is a very sensitive issue related to cloud and IoT security [11]. It happens when a malicious attacker has unauthorized access to the system or network to manipulate data. Malware attacks also cause data destruction.

Network Threats

Network security is an important factor in IoT and cloud, having weak network security leads to attacks, which include man-in-the-middle attacks and denial of service. IoT network security involves securing the communication network of different IoT objects.

Man-in-the-Middle attack

It is a form of account hijacking where an attacker steals the credentials of the user to get access to his account. The credentials are used to access and monitor the network causing interference in communication between the nodes. For more information on Man-in-the-middle attacks - feel free to read our article on the subject.

Denial of Service

DOS attacks are done to prevent legitimate users from accessing the IoT and cloud network, storage, data, and other computing services. DOS attacks also cause a delay in operations because many requests are made thus consuming more resources. For more information on Denial of Service attacks - please refer to our other article on the subject.

3. Related Work

Ngangmo et al. (2019) The Cloud of Things (IoT) that refers to the integration of the Cloud Computing (CC) and the Internet of Things (IoT), has dramatically changed the way treatments are done in the ubiquitous computing world. This integration has become imperative because the important amount of data generated by IoT devices needs the CC as a storage and processing infrastructure. Unfortunately, security issues in CoT remain more critical since users and IoT devices continue to share computing as well as networking resources remotely. Moreover, preserving data privacy in such an environment is also a critical concern. Therefore, the CoT is continuously growing up security and privacy issues. This paper focused on security and privacy considerations by analyzing some potential challenges and risks that need to be resolved. To achieve that, the CoT architecture and existing applications have been investigated [6]. *Christos Stergiou et al. (2018)* presented a survey of IoT and Cloud Computing with a focus on the security issues of both technologies. Specifically, we combine the two aforementioned technologies (i.e Cloud Computing and IoT) in order to examine the common features, and in order to discover the benefits of their integration. Concluding, we present the contribution of Cloud Computing to the IoT technology. Thus, it shows how the Cloud Computing technology improves the function of the IoT. Finally, we survey the security challenges of the integration of IoT and Cloud Computing [7] *Antonio Puliafito et al. (2015)* The secure boot-up and setup of Internet of Things (IoT) devices connected over the Cloud represent a challenging open issue. This paper deals with the automatic configuration of IoT devices in a secure way through the Cloud, in order to provide new addedvalue services. After a discussion on the limits of current IoT and Cloud solutions in terms of secure self-configuration, we present a Cloud-based architecture that allows IoT devices to interact with several federated Cloud providers. In particular, we present two possible scenarios, that is, single Cloud and a federated Cloud environments, interacting with IoT devices and we address specific issues of both. Moreover, we present several design highlights on how to operate considering real open hardware and software products already available in the market [8]. *Shynu P. G. et al. (2020)* develops a new method using Convergent and Modified Elliptic Curve Cryptography (MECC) algorithms over the cloud and fog environment to construct secure deduplication systems. The proposed method focuses on the two most important goals of such systems. On one side, the redundancy of data needs to be reduced to its minimum, and on the other hand, a robust encryption approach must be developed to ensure the security of the data. The proposed technique is well suited for operations such as uploading new files by a user to the fog or cloud storage. The file is first encrypted using the Convergent Encryption (CE) technique and then re-encrypted using the Modified Elliptic Curve Cryptography (MECC) algorithm. The proposed method can recognize data redundancy at the block level, reducing the redundancy of data more effectively. Testing results show that the proposed approach can outperform a few state of-the-art methods of computational efficiency and security levels [9]. *Chaima Gharbi et al. (2021)* proposed an integrated Fog Cloud-IoT architecture based on Multi-Agents System and Blockchain technology. Multi-Agents System has proven itself in decision-making aspects, distributed execution, and its effectiveness in acting in the event of an intrusion without user intervention. On the other side, we propose Blockchain technology as a distributed, public, authentic ledger to record the transactions. The Blockchain represents a great advantage to the next generation computing to ensures data integrity and to allows low latency access to large amounts of data securely. We evaluated the performance of our proposed architecture and compared it with the existing models. The result of our evaluation shows that performance is improved by reducing the response time [10].

4. Proposed Methodology

The main objective behind the proposed model is to preserve the privacy of the model so that the Cloud's data and services become more secure. The main focus of the proposed system is to secure two Ends properly in which one is the Services of the Cloud and another is the medium of communication between the User and the Cloud.

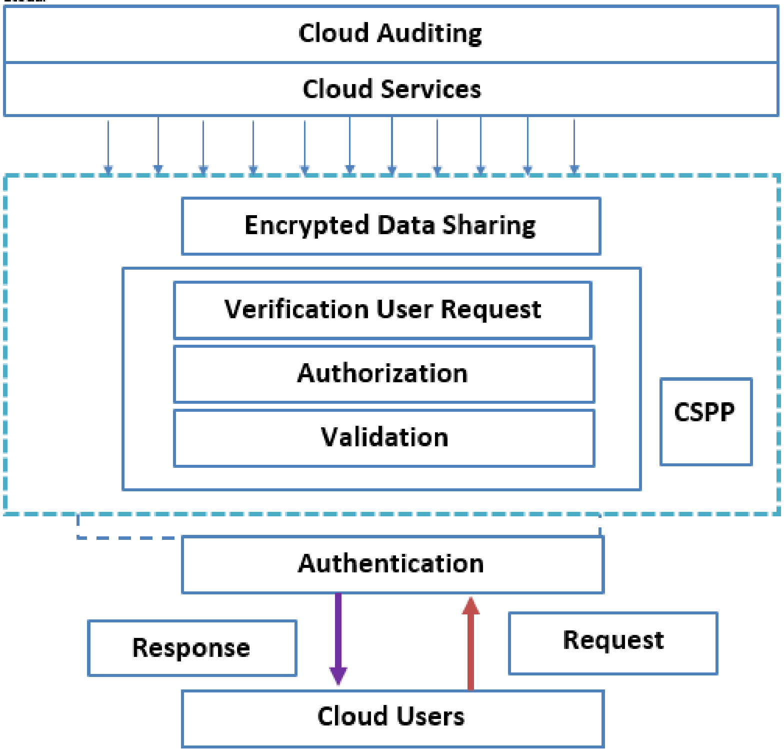


Fig. 1 Data flow diagram of proposed methodology

The main focus of the proposed model

1. Cloud's/Service's Privacy and security
2. Securing the communication medium

The proposed model has many components in it. The proposed CSPP model is working as an intermediate between the user and the Cloud Services. As the model is providing an efficient and secure model to Cloud for the preservation of privacy. The proposed CSPP model majorly focuses on the component of the system further in-depth we can use any specific kind of algorithm as per the Cloud computing power, Space requirements, and processing requirements. There are the following components in the Proposed CSPP Model. Let's have a look at the names first then we'll understand the working of each in-depth.

A components in the proposed CSPP Model

1. User Validation
2. User Authorization
3. User Authentication
4. User Request verification

5. Encrypted Data Sharing/ Encrypted Data Flow

Therefore, these are the components of the proposed CSPP Model. Every component of the model plays a vital role in preserving the privacy of the Cloud and helping the system to achieve a new level of security. Let's dive into every component and with the help of the flow of the process, we'll understand them.

User Authentication

User authentication is a very important part of any Cloud. It is the process of identifying the users that the user is a valid user or not. We can also say that in this Cloud simply recognize the user's identity. It is a method in which we associate every user with credentials and whenever the users request to access the credentials are always required just to make sure that the user is trusted and is genuine. All the safe credentials are saved by the server in an encrypted format so that anyone from the admin side can't see the credentials directly. Authentication is like the door in the building where the building represents the Cloud. So, if we need to enter the building, we need to clear that first door with the credentials. There are many different types of authentication techniques available in which the Cloud owner can use the wanted and affordable technique.

The authentication of the user needs to be done whenever the user wants to access the Cloud. So, this is about the user authentication in the system. The authentication is a very simple approach but it is the required most. It simply Filters out all the normal unwanted users.

User Authorization

Authorization is the second most vital process in the Cloud. It is a kind of Security mechanism. The whole process is simply granting and restricting the different users to access the resources and the services of the Cloud. Usually, this tells about the allowed access as per the user post in the organization. For example, when we talk about the Cloud of any organization then the receptionist only has a few accesses to portals and those are related to the work of receptionist only. But the clerk in the same company has different access to resources so every user in the Cloud has its own required and allowed access to the Cloud services.

When the model first confirms a allow by authentication then the users try to access the Cloud then the CSPP model makes sure that the service which users want to access is allowed to the user or not. If it is allowed then the user can process further else the user is simply blocked to proceed further and the session of the user will crash. The user is sent back to the authentication page if the user tries to access any unwanted data or services which are restricted to that particular user.

Mostly in Cloud's or system the access control combines of these two steps, only the First one is the authentication and another one is the authorization.

User Validation

Usually, the validation terms refer to checking something and acknowledging it with signals that it is right or not or we can also say that checking that it is valid or not. Here the validation terms refer to the Backend working of the Authentication and authorization of the user. here the validation also validates the user's physical address. This means whenever the new users try to access the Cloud and authenticate itself for the very first time with a new device then in the backend the user validation portal raises a request to the server that the device with this physical address wants to access the data. The server can be either of CSPP Model or the Cloud, so accepting or declining the request. Most of the requests are simply allowed by the system which is genuine and correct physical addresses. But on the server-side, the admin needs to do manual work for unusual physical address requests. In some organizations, they used to limit the device of the users too. However, in our proposed system this step will be done once every device. This kind of process will help us to keep the fake users (With unusual physical addresses) away from the Cloud and our system this will also help in increasing the security of the Cloud.

User Request verification

This is similar to the user validation but there the Proposed CSPP model is validating the physical address but here the Requested resources or services will be validated concerning the user from the very first time only. if any of the user clears all the three steps before this then this is the last process to complete the request. This also works in the backend of the user and one of the very important parts of the Proposed CSPP Model. Whenever any user tries to access the particular part of their Cloud or any particular portal for the very first time than the proposed model automatically raises a request to the admin that this particular user, with this identity and with this physical address wants to access that particular part of our Cloud. This is only the one-time process for every user. Once the admin will allow the user to do so, the user is able to access the required and desired resources. The major benefit of this kind of portal is the unwanted users who are fake can be avoided because they don't know about the internal working and requests. Cloud is usually for a closed organization so we can avoid the unwanted members by such a mechanism.

Encrypted Data Sharing/ Encrypted Data Flow

as all the above 4 components are playing their role in securing the server mostly. The second most important factor in preserving privacy in any system is the medium of communication or we can say that the communication Channel. Most of the issues raised are due to the data simplicity as mostly the data travels is in Normal human Readable form. Any of the attacker in between can simply read the data in between. However, in the proposed CSPP Model there is a system that encrypts the data, which need to transferred from the origin and decrypt it at the receiver end. This simply means if the user us sending the data to the Cloud then in backend the data is encrypted with the help of a random key generated for T time. when the request reached the destination and key are also been shared with the msg in a unique pattern, so the server simply decrypts the data and performs the required operation. The introduction of such things in Cloud may complex the working a bit but will lead to raising the security and privacy to a new and level up peaks.

Cloud auditing with IOT

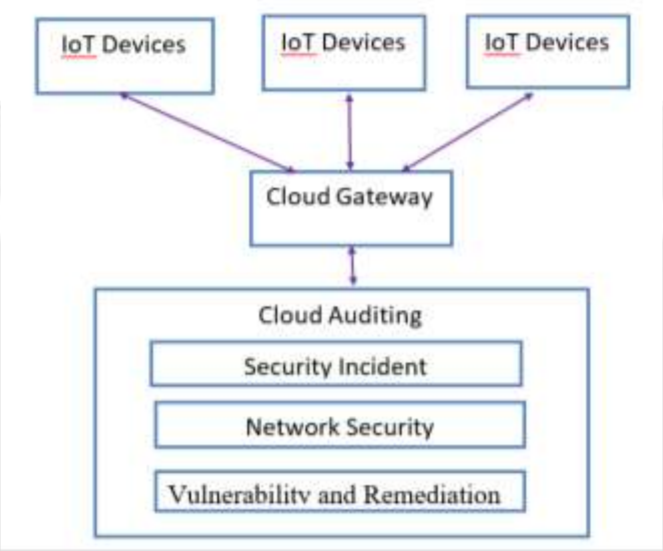


Fig. 2 Integrated framework for security using Cloud and IoT

The proposed model has a very unique and effective architecture. Before understanding the proposed work or the details about the proposed system, firstly let's have a look at the requirements of the industry or the expectation from the proposed work.

Requirement 1: As in any industry there are many devices and machinery and concerning the different profiles, we need the proper control over the Devices, so the IoT devices or the Edge device need to be controlled properly.

The above statement says that "The end Devices" is a big concern.

Requirement 2: As in any Industry, there is a number of users who have different requirements. So, there must be a proper GUI that provides the above thing properly.

The above statement says that "User management" is also a big concern.

Requirement 3: As in industry, there is a need for efficient handling of data from Cloud and IoT Devices so that the data can be maintained properly and efficiently.

The above statement says that "UI Reporting" is also a big concern.

Requirement 4: As many industries have either already designed application or there is some third party, tool we need to connect to the system, so there must be a portal, which maintains the business integration with others.

The above statement says that "Integration" is also a big concern.

Requirement 5: When we are working with the hardware, we have a different platform/language and similarly when we are working for the Cloud, we have different platform/Language so we need a gateway, which integrates these two only.

The above statement says that "Cloud gateway" is also a big concern.

Requirement 6: In some industry, the work or the production line is monotonous that means we need to do the same task repeatedly so there we need a system, which can itself train from the working and after t time it must be capable of repeating the work.

The above statement says that "Machine Learning" is also a big concern.

As these are the requirements of the system, means these must be there in the combined approach of the Clod + IoT. So, taking these in reference let’s try to understand the proposed approach or proposed model.

Component 1: IoT Device/IoT edge Devices.

As in any kind of industry or any kind of organization, there are devices or machinery over which we need a smart and mobile control, or sometimes we need to monitor the particulars. The end devices can be named as IoT devices/IoT edge Devices.

Component 2: Cloud Gateway

As till now, we are working with hardware only so after all the hardware we need to combine the data in a portal and connect the particular portal with the main Cloud of the system. So there is a need to Cloud gateway which is completely bi-directional in working. Whenever Actions request the data from things it flows that side and vice versa. So majorly it helps in the connectivity of hardware data to the main and only space of the system. It is just a door between the devices and the software.

Component 3: Cloud Auditing

In a Cloud computing audit, a variation of these steps is completed in order to form an opinion over the design and operational effectiveness of controls identified such as security incident, network security and Vulnerability and remediation management. In the proposed framework of Cloud and IoT for providing security to our system we use SHA security technique. The working of secure hash algorithm is discussed above.

5. Experimental Setup and Result Analysis

5.1 Simulation Environment

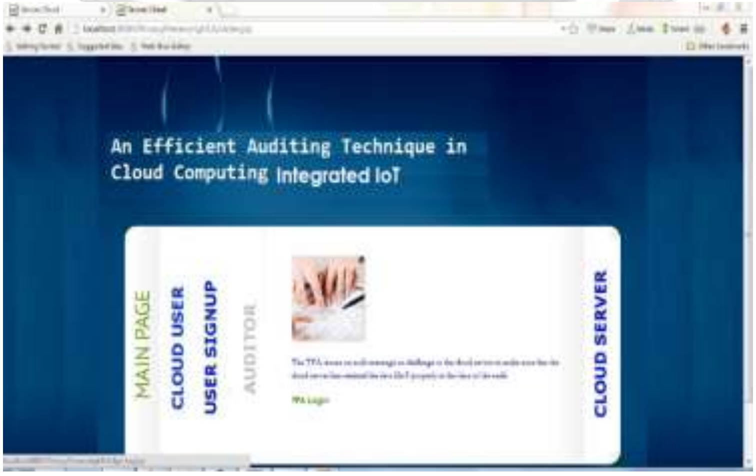
Simulation is the piece of hardware or software that speculates the behavior of the network without presenting actual network. In cloud computing research, cloud simulation is a technique which evaluates the behavior of the cloud by calculating the interaction between various cloud computing devices or by mathematical formulas. In simulators, cloud is modeled with various devices, links, and applications and then it is analyzed to evaluate the performance of it. Users can also customize the cloud simulators to acquire their specific analysis requirements.

Our work having following requirements for simulation in the cloud computing:-

A. Cloud Simulator (We Used CloudSim API & Apache Server For Cloud Simulation)
B. Development Environment (jdk or NetBeans)
C. Database

5.2 Experimental Setup Framework

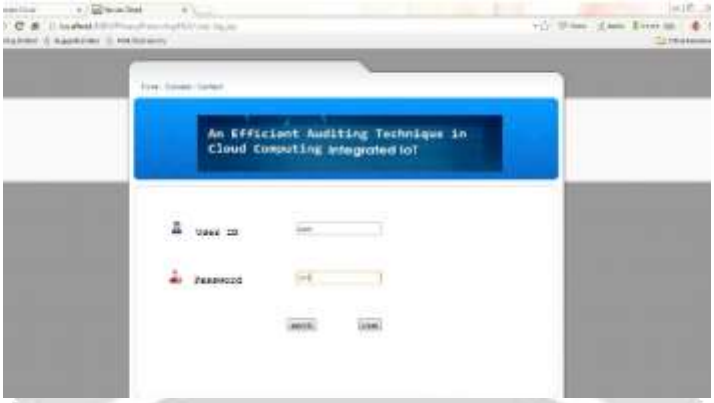
As per the understanding of scenario we have further establish the Apache framework using Java language and JSP framework. Thus in order to execute the framework and description is given below by step that is performed in our work.



An Efficient Auditing Technique in Cloud Computing Integrated IoT

Fig.3 Apache framework for experiment analysis module page.

In the figure above the modules are shown where we have taken cloud user module where user can sign up and login further to login their account and access their data or store their data in secure encrypted format. Also the TPA module is described using which the third party is shown which is responsible for verification and management. The third is cloud admin center which can able to see the files available with the cloud.



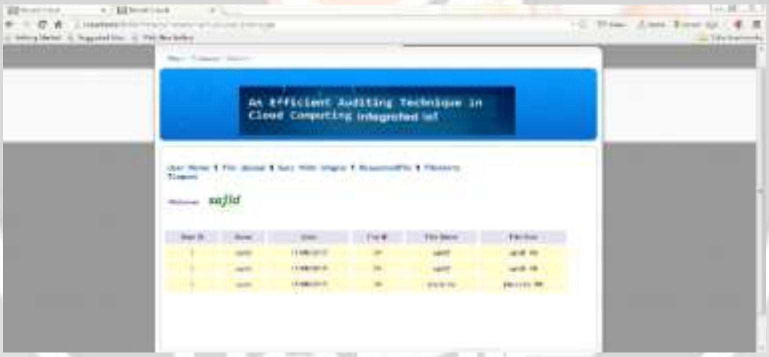
An Efficient Auditing Technique in Cloud Computing integrated IoT

User ID

Password

Fig.4 Login Module for TPA, User and cloud center

In the figure above the complete login module is described using which the either party can login in to their registered account, as the authentication and authorization is performed in this module for all the user account type.

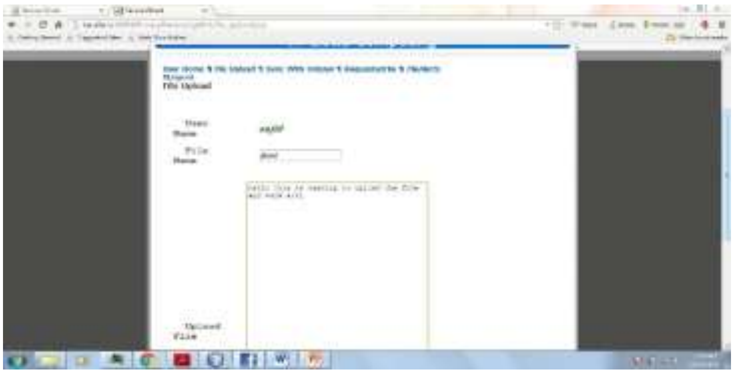


An Efficient Auditing Technique in Cloud Computing integrated IoT

sajid

Fig.5 User Login home and File Storage and view module

In the figure above the show is all the stored user data , file name, file id, user id, file size and other required component which identify a file separately is given into this figure and the further in menu file upload, update, requesting for the audit, file security alerts are also kept . as per the requirement user can go in either option to operate account.



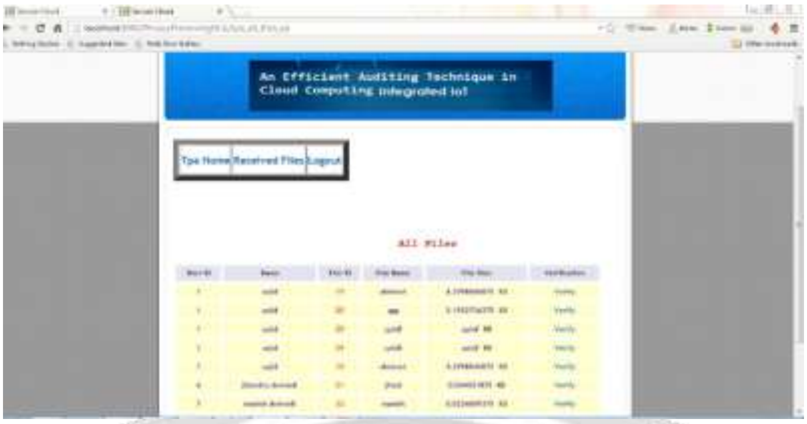
File Upload

sajid

Upload File

Fig.6 File upload module

In the figure described above the files identity and upload module is considered where the data can be taken and further can upload in the encrypted form on cloud data center. This module is required for user to store secure data into the cloud server.



An Efficient Auditing Technique in Cloud Computing integrated IoT

All Files

Fig.7 TPA home and verification module

The figure described above is the module from TPA third party authentication side where TPA can check the available data and files in the system. Also in this module the data verification option is given that verify the file data using hash function and also it gives the proper alerts to the user. This module produce a system where tpa send challenge to the cloud party and receive the response as the file is available safe or not.

5.3 Result analysis

As the requirement of the system and implemented by us here is the comparison analysis is made based on the keysize, server computation time, TPA computation time where the system proven our proposed scenario as best among the available technique.

Table 1 – comparison in terms of hashing key value

Algo/Parameter	SHA0	SAH-1	SHA-2	SHA-3
output size	160	160	256	512
internal state	160	160	256	1600
block size	512	512	512	1152

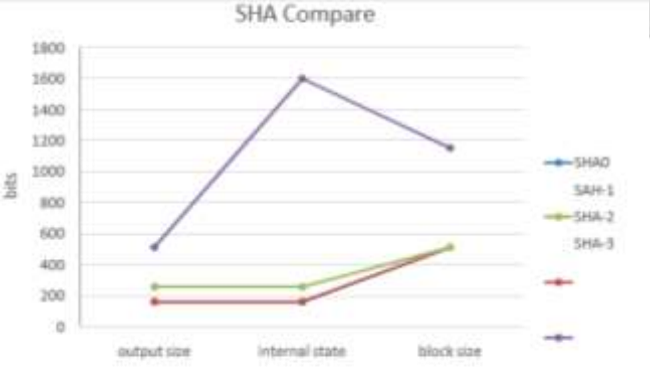


Fig. 8 – Graphical Analysis of hashing key system

6. Conclusion and Future Work

In this paper, we involve in the field of IoT based cloud security such as encryption technique to store data and unauthorized access to the data. Also our work in this paper discuss about the literature work has been performed in the cloud-IoT security. The motivation for the work is to find a best technique which take a less time and provide high security to the encrypted data store in cloud-IoT system. The considered existing and proposed work were performed and implemented using Java Apache Framework and Arduino and thus the result were monitored using different considered parameter. As per our observation the proposed algorithm is efficient and reliable in terms of encryption scheme which follow symmetric key encryption and also in case of integrity verification which is the latest hashing SHA volume to prove and execute our system over the existing algorithm. The security and integrity verification in cloud is always required as the number of users and portals are switching their workspace to the cloud environment instead of traditional server configuration. thus our work in this field lead the solution to store and verify the originality of available scenario.

Reference

[1] Jayant D. Bokefode, Avdhut S. Bhise, Prajakta A. Satarkar and Dattatray G. Modani, "Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption", Twelfth International Multi-Conference on Information Processing-2016 (IMCIP-2016), Procedia Computer Science 89 (2016) 43 – 50.

[2] Singh et al. "Cloud Computing Security Issues, Challenges and Solutions", EasyChair Preprint, 2020.

[3] Rashmi Singh and H Singh," Exposure And Avoidance Mechanism Of Black Hole And Jamming Attack In Mobile Ad Hoc Network" International Journal of Computer Science, Engineering and Information Technology, Volume 7, No. 1, 2017

[4] Murali Gopal et al., "Design and Implementation of an Algorithm for Mitigating the Congestion in Mobile Ad Hoc Network", International Journal on Emerging Technologies 2019, Vol 10, Issue 3 Page 472-479.

[5] Muhammad Kazim and Shao Ying "IOT and Cloud Computing Security Threats", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 3, 2015

[6] Ari, A. A. A., Ngangmo, O. K., Titouna, C., Thiare, O., Kolyang, Mohamadou, A., Gueroiu, A. M. (2019), "Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges" Applied Computing and Informatics, Vol. ahead-of-print No. ahead-of-print. https://10.1016/ j.aci.2019.11.005. The original publication date for this paper was 22.11.2019.

[7] Christos Stergiou , Kostas E. Psannis, Byung-Gyu Kim , Brij Gupta , "Secure integration of IoT and Cloud Computing", Future Generation Computer Systems, 78, 964–975. doi: 10.1016/j.future.2016.11.031.

[8] Antonio Puliafito, Antonio Celesti, Massimo Villari, and Maria Fazio, "Towards the Integration between IoT and Cloud Computing: An Approach for the Secure Self-Configuration of Embedded Devices", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2015, Article ID 286860, 9 pages.

[9] Shynu P. G. , Nadesh R. K. , Varun G. Menon, Venu P., Mahdi Abbasi and Mohammad R. Khosravi, "A secure data deduplication system for integrated cloud-edge networks", Journal of Cloud Computing: Advances, Systems and Applications (2020) 9:61.

[10] Chaima Gharbi , Lobna Hsairi and Ezzeddine Zagrouba " A Secure Integrated Fog Cloud-IoT Architecture based on Multi-Agents System and Blockchain", In Proceedings of the 13th International Conference on Agents and Artificial Intelligence (ICAART 2021) - Volume 2, pages 1184-1191 ISBN: 978-989-758-484-8

[11] N Salimath, S Mallappa, N Padhy, "Scrambling and descrambling of document image for data security in cloud computing", Smart Intelligent Computing and Applications, 283-290.

[12] BS Thakur, "Analyzing a Cattle Health Monitoring System Using IoT and Its Challenges in Smart Agriculture" Intelligent System Design, 837-843