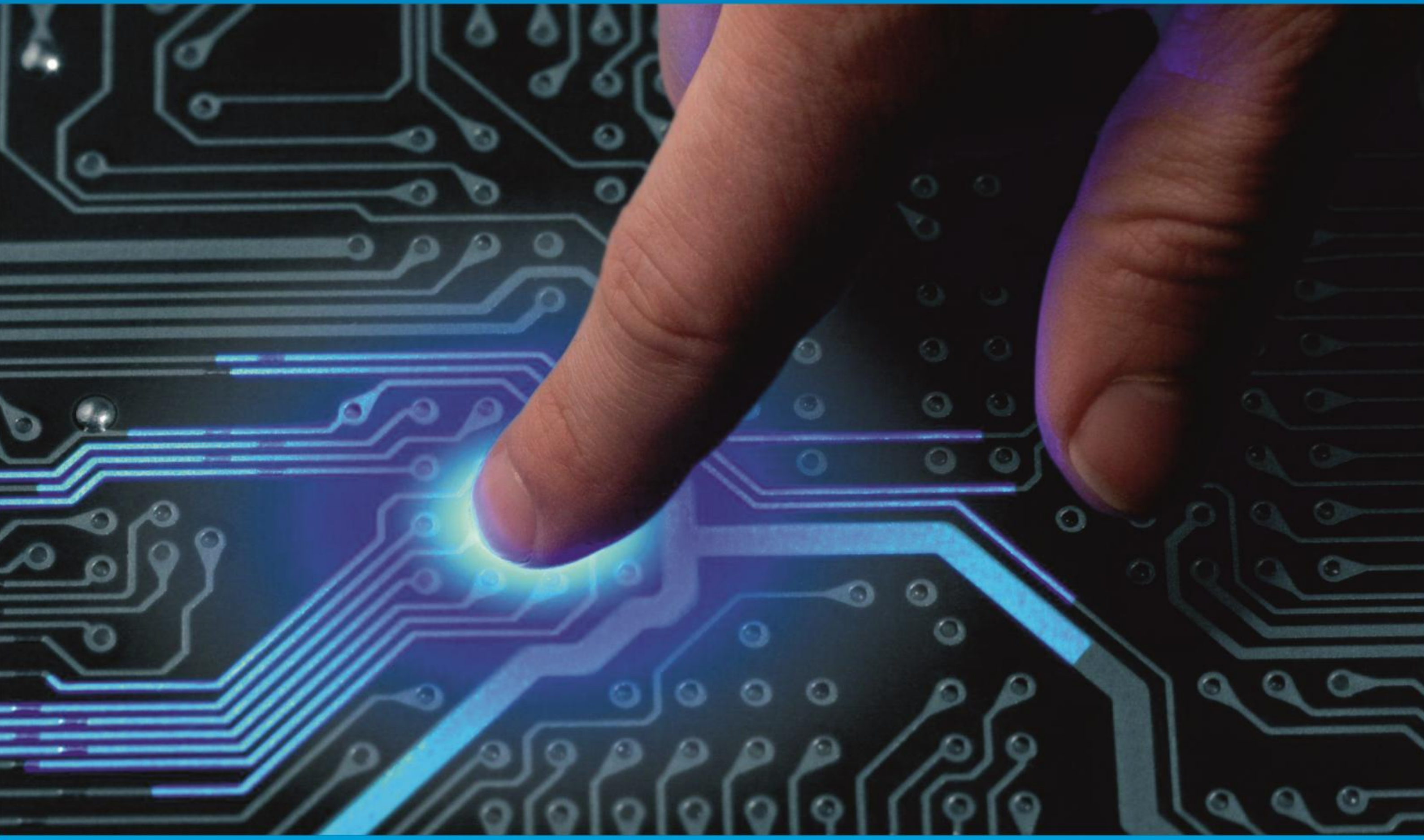
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903218 |

Revocable Storage Identity Based Encryption

Mohanraj P[1], Nirmal Kumar M[2], Somasundaram N[3], Mrs. B.M.Brinda[4]

Department of Computer Science and Engineering, Paavai College of Engineering, Namakkal, India[1]

Assistant Professor, Department of Computer Science and Engineering, Paavai College of Engineering, Namakkal, India[2,3,4]

ABSTRACT: Cloud computing is a disruptive technological paradigm for providing on-demand access to data and applications from anywhere at any time Cloud computing involves storing data, temporarily or on a more permanent basis, over the Internet. In the last decade, many organizations have turned to cloud solutions for storage or back up to facilitate productivity and save money [30]. "The Cloud" is a concept used to describe the virtual nature of digital storage, which can mean the data are stored on servers physically placed in many geographical locations. Considering the proliferation of cloud storage as a cost-effective way to save large amounts of data, healthcare organizations are cautioned that not all cloud storage services are created equal. It is important to conduct a privacy risk assessment prior to signing on to a cloud computing service to confirm the healthcare organization will still be in compliance with privacy legislation. For instance, an organization may be required to store personal information within its jurisdiction and the cloud storage resides outside of this area. PIA and STRA are required to assess risk, and mitigation strategies may include data encryption in transit and storage, data segregation to ensure an organization retains custody and/or control of the personal information, strong authentication and access rules, vendor service levels that provide downtime procedures and data recovery timelines, and the ability to extract the organization's data at termination of the contract. Cloud service providers should be able to provide audit reports of user access and produce an audit log report if required during a privacy or security investigation. When a cloud service is used by a healthcare organization to collect personal information from a patient/client through an online process, this is considered a new collection and will require a consent mechanism.

KEYWORDS: cloud based data sharing, access control, cloud storage service, intel SGX, identity basrd encryption, Revocable storage service

I.INTRODUCTION

Big Data' is a term used for massive collection of data that is huge in size and growing exponentially with time. The data is being generated from several sources such as Social media, usage of Search engines, Sensors, Banking transactions, Financial applications etc., and that data may be structured, unstructured or semi-structured. Big data is so large and complex that none of the traditional data management tools are able to store or process it efficiently. In modern information technology, big data is a term applied to data sets whose size is beyond the ability of commonly used software systems to store, manage, and process within a tolerable elapsed time. Big data sizes are a constantly moving target, currently ranging from a few dozen terabytes to many peta bytes of data in a data center. A data center mainly focuses on the storing and processing of big data sets, real-time data mining, and streaming media delivery etc. Data-intensive applications and research will be integral to many future scientific endeavors, but will demand specialized security mechanisms to make data centers efficient and secure. In addition, the research community now has the option of accessing storage and computing resources on demand, and the IT industry is currently building multiple big data centers for social networks and applications. Consequently, large amounts of clients' private and secret data (including meta-data) will be stored in data centers, and will need protection during processing and transmission. Thus, data centers should be able to provide efficient security, access, and update mechanisms to not only huge files running into peta bytes, but also to small files that are only a few hundred bytes. In all the above cases, determining how to de-sign a secure and efficient scheme for tenants to access their data on the data center storage is crucial. Many different approaches have emerged to deal with various attack vectors within the information system. These methods include "firewalls", "intrusion detection systems", "intrusion prevention systems", "virus "scanning programs", "access control mechanisms", and "real-time monitoring". Each method emphasizes the specific range and type of potential attack vectors. In addition, the architecture, technology, and requirements of the management information system require stringent cyber defense methods. Specifically, ensuring the security of a single component defines a significantly different problem than a homogeneous cloud computing architecture. In particular, cloud computing architecture derives several unique attributes in its many forms. These include, but are not limited to, joint needs for multi-tenancy, dynamic lease, multiple operational domains, shared infrastructure, and policy definitions. These attributes need access control mechanisms that similarly promote these attributes.

1.1 Contributions

In this paper we designed To prevent the leakage of the data owner's protected data to unauthorised entities, afteraccess is given to one or more authorised data consumers (or recipients).The dataowner should be able to provide access to a large amount of recipients while also beingable to efficiently and effectively revoke recipients from data access, at any time.The protected data should also be accompanied by a policy that states who, what, where, whenand how the data is to be accessed. The policy should be enforced during the lifetime ofthe protected data.In other words, a data owner should be able to share his or her data with millions ofusers whilst ensuring that it is protected from unauthorised access and usage. The datashould remain encrypted from any unauthorised user or Cloud insider. The data ownershould also be able to revoke a user's access on-the-fly, without having to re-encrypt and redistribute keys. Thus, key management needs to be efficient.In addition, the data owner should be able to specify a policy that enforces how the data is to be used by the authorised data consumer. The data owner can use the policy to enforce a wide variety of complex conditions. For example, a policy could state that " the data can only be accessed by students for five days" or "the data can only be read,but cannot be copied, modified or printed."This gives the data owner greater access control over their data. We now provide a formal description of the above problem statement. We consider a data owner do ∈O where O represents the set of all possible users. The do creates data∈D where D represents all possible data. The data D can be distributed and accessed by data consumers dc∈C where C is a subset of Ochosen by the do. We now provide the following restrictions:

1. The data D cannot be accessed by any entity outside ofC.

2. The data D cannot be accessed bydc, without the permission of data ownerdo.

3. The data owner do can give permission to one or more data consumers D c∈C to access the data D.

4. The data owner do can revoke the access of data consumer DC to the data D

5. If a policy p∈Pis associated with the data D and the data owner do gives permission to the data consumer DC, D can be accessed by DC as long aspisobeyed.

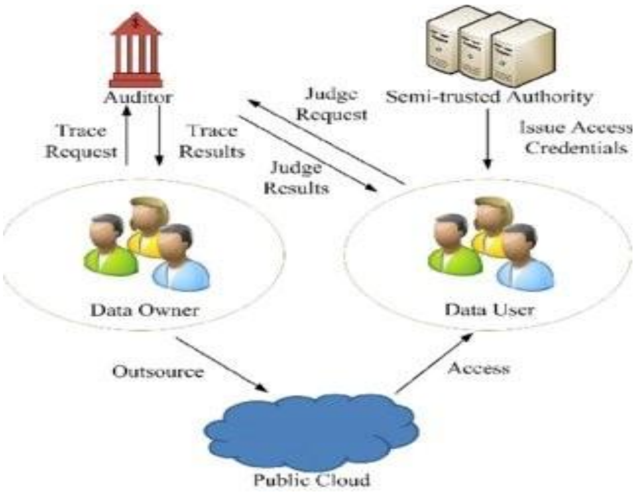
1.2 Organization

The rest of the paper is defined as follows. Section 2 introduces the preliminaries needed. Thearchitecture and security of the system are given in Section 3. In Section4 and 5 the proposed systems and security analysis is defined. Performance evaluations is in Section 6. andSection 7 describes conclusion and futurework.

II.SYSTEM MODEL

2.1 Frame work

We consider a dual access control system for revocable storage identity based encryption system with fiveentities, as designed in Fig. 1: auditor(enclave) ,data owner, data user, key authority and cloud server



Authority is responsible for initializing system parameters and data user registration. Also, it handles the call request from the cloud in the first proposed construction.
•Data owner holds the data and wants to outsource his data to the cloud. In particular, data owners (only) want to share their data with those who satisfy certain conditions (e.g., professors or associate professors). They will be offline once their data have been uploaded to the cloud .
•Data user wants to download and decrypt the encrypted data shared in the cloud. Those who are authorized can download the encrypted file and further decrypt it to access the plaintext.
•Cloud provides convenient storage service for data owners and data users. Specifically, it stores the out-sourced data from data users and handles the down-load requests sent by data users.
•Enclave handles the call request from the cloud (used in the second system).The description of workflow is introduced as follows. Data owners encrypt their data under the access policies chosen by themselves and upload the encrypted data to the cloud. Authorized data users can download the shared data by sending a download request to the cloud. Upon receiving a download request from an authorized data user.

2.2 EXISTING SYSTEM

In the existing system, it has been proposed a framework to remove the problem of single-point performance bottleneck and provide a more efficient access control scheme with an auditing mechanism with single CA for key generation and distribution, who is assumed to be trust worthy and multiple attribute authorities for client authenticity verification.

2.2.1 DRAWBACKS OF EXISTING SYSTEM

The cloud computing does not provide control over the stored data in cloud data centers. The cloud service providers have full of control over the data, they can perform any malicious tasks such as copy, destroying, modifying, etc. The cloud computing ensures certain level of control over the virtual machines. Due to this lack of control over the data leads in greater security issues than the generic cloud computing model as shown in figure 1. The only encryption doesn't give full control over the stored data but it gives somewhat better than plain data. The characteristics of cloud computing are virtualization and multi tenancy also has various possibilities of attacks than in the generic cloud model. The figure 2 has various issues those are discussed below in clearly. Attacks that come from external origins are called outsider attacks [30]. Data security is one of the important issue in cloud computing. Since service providers does not have permission for access to the physical security system of data centers. But they must depend on the infrastructure provider to get full data security. In a virtual private cloud environment, the service provider can only specify the security setting remotely, and we don't know exactly those are fully implemented. In this Process, the infrastructure provider must reach the following objectives: (1) confidentiality, for secure data transfer and access, and (2) audit ability [31]. So that outside intruders can't access sensitive data which is stored in cloud. After moving to cloud computing environment, there are many issues in geographic jurisdictions, regulatory law, performance assurance, contract enforcements, etc.

2.3. PROPOSED SYSTEM

In the proposed system, it has been proposed a novel framework to improve the security of the system along with single CA and multiple AAs and auditing mechanism, an observer machine is added in the system which monitors CA for its behaviour. It checks whether CA is doing anything else other than what it has claimed to do. If observer finds any discrepancy then it generates a report regarding it. Then a new CA has chosen among AAs. In this system there is no separate CA, instead, CA is chosen among AAs and CA is not assumed to be trustworthy. This system along with solving the problem of single point bottleneck in case of performance and efficiency makes the system more secure.

2.3.1. ADVANTAGES OF PROPOSED SYSTEM

After moving to cloud computing environment, there are many issues in geographic jurisdictions, regulatory law, performance assurance, contract enforcements, etc. The above mentioned issues are comes under the legalities, Service Level Agreements and data location in data centers .The integrity and confidentiality of data and services are related with access control and identity management. It is important to maintain track record for user identity for avoiding unauthorized access to the stored data. The identity and access controls are complex in cloud computing because of that data owner and stored data are at different executive platforms. In cloud environment, different organizations use variety of authentication authorization agenda. By using different approaches for authentication and authorization gives a compound situation over a period of time. The cloud resources are dynamic and are elastic for cloud user and IP addresses are continuously changed when services are started or restarted in pay per usage model. That allows the cloud users to join and leave feature to cloud resources when they required i.e., on-demand access policy. All these features need efficient and effective access control and identity management. The cloud has to maintain quickly updating and managing identity management for joining and leaving users over cloud resources.

III.OUR CONSTRUCTION

3.1PRIVACY-PRESERVATION FOR SENSITIVE DATAIN CLOUD COMPUTING:

Over the time, organizations have collected valuable information about the individuals in our societies that contain sensitive information, e.g. medical data. Researchers need to access and analyze such data using big data technologies in cloud computing, while organizations are required to enforce data protection compliance .There has been considerable progress on privacy preservation for sensitive data in both industry and academia, e.g., solutions that develop protocols and tools for an encryption of data for confidentiality purposes. This section categorizes work related to this area according to different privacy protection requirements. However, these solutions have not yet been widely adopted by cloud service providers or organizations. Pearson [1] discusses a range of security and privacy challenges that are raised by cloud computing. Lack of user control, lack of training and expertise, unauthorized secondary usage, complexity of regulatory compliance, trans border data flow restrictions and litigation are among the challenges faced in cloud computing environments. In the authors describe the privacy challenges of genomic data in the cloud including terms of services of cloud providers that are not developed with a healthcare mindset, awareness of patient to upload their data into the cloud without their consent, multi-tenancy, data monitoring, data security and accountability. The authors also provide recommendations for data owners when aiming to use cloud provider services. In the authors discussed several privacy issues associated with genomic sequencing. This study also described several open research problems (such as outsourcing to cloud providers, genomic data encryption, replication, integrity, and removal of genomic data) along with giving suggestions to improve privacy through collaboration between different entities and organizations. In another effort raw genomic data storage through encrypted short reads is proposed. Outsourcing privacy is another topic that is discussed .The authors define the concept of “outsourcing privacy” where a database owner updates the database over time on un trusted servers. This definition assumes that database clients and the un trusted servers are not able to learn anything about the contents of the databases without authorized access. The authors implements a server-side indexing structure to produce a system that allows a single database owner to privately and efficiently write data to, and multiple database clients to privately read data from, an outsourced database. Homo morphic encryption is another privacy-preserving solution that is based on the idea of computing over encrypted data without knowing the keys belonging to different parties. To ensure confidentiality, the data owner may encrypt data with a public key and store data in the cloud. When the process engine reads the data, there is no need to have the DP’s private key to decrypt the data. In private computation on encrypted genomic data, the authors proposed a privacy-preserving model for genomic data processing using homomorphic encryption on genome-wide association studies.

Important Security Issues in the Cloud:

Even though, the virtualization and Cloud Computing delivers wide range of dynamic resources, the security concern is generally perceived as the huge issue in the Cloud which makes the users to resist themselves in adopting the technology of Cloud Computing. Some of the security issues in the Cloud are discussed below: Integrity: Integrity makes sure that data held in a system is a proper representation of the data intended and that it has not been modified by an authorized person. When any application is running on a server, backup routine is configured so that it is safe in the event of a data-loss incident. Normally, the data will backup to any portable media on a regular basis which will then be stored in an off-site location .Availability: Availability ensures that data processing resources are not made unavailable by malicious action. It is the simple idea that when a user tries to access something, it is available to be accessed. This is vital for mission critical systems. Availability for these systems is critical that companies have business continuity plans (BCP"s) in order for their systems to have redundancy .Confidentiality: Confidentiality ensures that data is not disclosed to unauthorized persons. Confidentiality loss occurs when data can be viewed or read by any individuals who are unauthorized to access it. Loss of confidentiality can occur physically or electronically. Physical confidential loss takes place through social engineering. Electronic confidentiality loss takes place when the clients and servers are n " t encrypting their communications

3.2 CLOUD EDGE ORIENTED COMPUTING

Edge computing aims to deliver compute, storage, and bandwidth much closer to the data sources and/or end users. Though research on edge-oriented computing is still in its infancy and we lack a universally accepted open standard, there are a number of definitions of edge computing available, e.g., Shi et al. say that edge computing refers to the enabling technologies allowing computation to be performed at the edge of the network. Zhang et al. say edge computing is a novel computing model that allows the storing and processing of data at the edge of the network, and provides intelligent services near to the source of the data by collaborating with cloud computing. A similar concept to edge computing is fog computing, which was first proposed by Cisco, and aimed at extending cloud computing to the edge of network Vaquero and Rodero-Merino defined “fog computing is a scenario where a huge number of heterogeneous (wireless and sometimes autonomous) ubiquitous and decentralized device without the intervention of third parties. These tasks can be for supporting basic network functions or new services and applications that run in a sandboxed environment. Users leasing part of their devices to host these services get incentives for doing so". There is no clear distinguishing feature between fog computing and edge computing, since both push the intelligence and processing capabilities out of a centralized infrastructure into the logical extremes of the network close to the data sources and end users. But from the resource management point of view, the Fog, compared with the Edge, is a highly virtualized platform that provides computation, storage, and networking services between end devices and cloud computing data centers. In most identifiable scenarios, fog computing is often used when the task is service oriented, while edge computing occurs more if it is as an analytical task. From a hierarchical design view, the Fog is located between the Cloud and the Edge, such that a cloud-fog-edge three-tiered architecture has been recognized in many prior works. In general, edge-oriented computing can bring three prominent benefits to end users. First, reduce latency: the latency to the end user can be lower than it would be if the compute was farther away. Second, mitigate bandwidth limits: the ability to move workloads closer to the end users or data collection points reduces the effect of limited bandwidth at a site. This is especially useful if the service on the edge node reduces the need to transmit large amounts of data to the core for processing. Third, increase security: data can be pre-processed and protected before it is transferred to the cloud.

3.3 CLOUD-EDGE SECURITY:

Even though cloud-edge computing can bring a number of benefits compared with pure cloud computing, nevertheless, as edge devices proliferate, new attack vectors are emerging that take advantage of the proliferation of end points. Zhang et al. surveyed the recent research of data security in the field of edge computing, which pointed out that the security of outsourcing data is still a fundamental issue in edge computing data security. Their review work comprehensively covers the research focusing on data security, i.e. confidentiality, integrity, availability, authentication, authorization, and privacy preservation. Controlling access to data is well researched, and a standard has been defined for this: XACML .Our research makes use of this standard by employing an enhanced XACML policy decision point (PDP) to enforce our Data Sharing Agreement (DSA) policies. Our proposal for sharing CTI data covers all the issues mentioned by Zhang and is based on research by Carniani et al that proposed the design and implementation of a Usage Control Service to regulate the usage of resources in a Cloud IaaS service. They enhanced an XACML PDP to achieve this and integrated their solution into the Open Nebula Cloud platform. Henze et al. proposed a trust point, which is a local security-enhanced gateway at the border of a sensor network, that processes the sensor data before outsourcing it. In this trust point-based security architecture, the authors specified three trust domains: the fully trusted producer domain, containing the sensor nodes, the gateway devices and the data owner; the semi-trusted storage domain, including the cloud and cloud providers, who are assumed to be an honest-but-curious adversary; the un trusted consumer domain, consisting of entities such as services and service providers. Furthermore, the authors presented security solutions to address: the communication channel between the sensor network and the cloud, data confidentiality and privacy preservation for outsourcing the sensor data, and controlling access to the outsourced sensor data. However, their work had a static trust model and did not take into account different data protection mechanisms for different trust domains. In comparison, we assume a dynamic trust model, with user specified data protection mechanisms. The existing approaches for provably secure outsourcing of data and arbitrary computations are either not scalable (e.g. tamper-proof hardware based) or not efficient (e.g. fully homomorphic encryption). Consequently, the Twin Clouds architecture [21] was proposed, consisting of a trusted private Cloud and an untrusted public Cloud. They apply the concept of garbled circuits to protect data and computation instructions in the public Cloud. The trusted private Cloud is used to encrypt data and computation instructions. Then the protected computation instructions can be securely processed in the public Cloud. The drawbacks of this approach are that the computation instructions can only carry out simple operations and they have to be re-encrypted by the private Cloud after each execution. Pearson et al. proposed a data management solution for protecting data in the Cloud that focuses on fine grained access control of the outsourced data by attaching a sticky policy to the data, which states how and under which circumstances the data can be accessed. This is similar t Journal Pre-proof o our work. However, their trusted policy enforcement

point requires the establishment of a trust metric for all external entities, rather than this being controlled by the user, as in our work. Martin. proposed a general model for a privacy aware collaborative information sharing and analysis system. This approach can calculate a trade-off score on privacy gain and data utility loss over the privacy preserving mechanism. The trade-off score leads to optimizing the analysis result with regard to the balance between privacy and accuracy. However, this paper only considered either a fully centralized (i.e. cloud) or fully distributed/P2P (i.e. edge) architecture, rather than the more practical hybrid (cloud-edge) architecture, with different trust domains, which is a feature of our work. Several authors propose to process the data locally and only utilize the cloud for storage of sanitized data. They cannot benefit from the computation resources provided by the cloud but they can guarantee that neither the cloud provider nor any other unauthorized third-parties can access their sensitive information. In comparison, our data security model is tailored towards not only storage but also processing in the cloud.

3.4 CTI Data Sharing:

Sharing of CTI within a consortium or collection of similar organizations can be extremely beneficial because the member organizations often face common threats that are targeted towards similar type of systems, services and data. Cyber-security will be more effective if these organizations could work together to detect or prevent cyber threats facing them. Such collaboration helps in reducing risks faced by both the individual organization as well as the whole collective. Some basic methods of sharing CTI include public publishing of security alerts NVD vulnerability advisories ,and security vendors' security bulletins. A more extensive list of potential CTI is given in the CWE , CVE,and CVSS listings. Although all of these solutions and services share valuable information with the consumers, it is a one-way approach and most organizations do not or cannot easily reciprocate by sharing their CTI with these services. Some cyber-security solutions do exist that are more closely related to our work, both in the proprietary and public domains. Proprietary solutions, like BT Security Threat Monitoring, monitor and collect security events from their customers. However almost without exception, the collated data is not shared with anyone. In the public domain, there were EU projects like Coco-Cloud that enabled cloud users to securely and privately share their information. Similarly, CIF is a CTI management system that supports aggregation, processing and sharing of CTI, but does not have any capabilities for addressing the sensitive nature of some CTI data by using anonymization or encryption techniques. Zhou et al. surveyed collaborative intrusion detection systems (CIDS) that address coordinated attacks. Such attacks (e.g. large-scale scans, worm outbreaks and DDoS attacks) often occur simultaneously in multiple networks. Consequently, sharing alert data in CIDS can bring a global view and collaborative analysis results to the users. The main research challenges are alert correlation algorithms and appropriate CIDS architectures, which were categorized as centralized CIDS, hybrid CIDS and fully distributed CIDS, which are similar to our deployment models described later. Both Lo et al. and Shu et al. proposed using CIDS to detect DDoS attacks to Cloud Computing, whereby one regional IDS shares its alert data with the other IDS systems. This can help to reduce the overall computational costs of detecting the same attacks in multiple IDS systems and therefore improves overall detection rates. The difference between them is that Lo uses the fully distributed architecture while Shu uses the hybrid architecture. Furthermore, Shu proposed using a Back-Propagation Neural (BPN) network to detect unknown attacks. The utility and analysis accuracy of shared CTI data are obviously based on the utility of the CTI data obtained from the different sources. Clear text data has most utility, but sharing this often results in privacy leaks, since the CTI may include sensitive information that should not be shared with the other untrusted or unauthenticated partners. There has been plenty of research investigating privacy-preserving data sharing .Fung et al. proposed the privacy preserving data publishing approach in order to optimize the trade-off between data utility and privacy. Different security requirements and metrics often lead to the use of distinct privacy-preserving data mining techniques .Thus, it is necessary to have a flexible privacy-preserving data sharing model that can address the trade-off between data privacy and data utility, whilst taking into account the different levels of trust that collaborators have in each other. This is a subject of our research. Traditional storage means a specific storage device, or the assembly constituted by the large number of the same storage device. In using traditional storage, you need a very clear understanding of some of the basic information of the storage device, such as device type, capacity, supported protocols, transmission speed. In addition, regular maintenance of the equipment, hardware and software updates and upgrades need to be considered separately. Although cloud storage is composed by a large number of storage devices, storage devices can be heterogeneous and cloud storage users do not care about the basic information of the storage devices and its location. In cloud storage, issues such as equipment failures, equipment updates and upgrades were also be full considered, and can provide more reliable service. The core of cloud storage is the combining of application software with storage device, to achieve the changes from storage device to storage service by application software. It's not directly to use storage devices but the Data Access Service provided by the entire cloud storage system for users. So in the strict sense, cloud storage is not storage but a service. Cloud storage provides directly data storage services for end users and indirect data access in application system, and other forms of service, with many service forms of network hard drive, online storage, online backup and online archive storage service

In Cloud storage, data were distributed to plurality nodes of multiple disks, so the system needs simultaneously high-speed read and write to multiple disks. The speeds of disk data read and write should be prioritized after the basic problems of storage capacity in cloud storage architecture design. In fact, larger disk capacity can be obtained by combining multiple disks, along with the continued expansion of the hard disk capacity as well as hard drive prices continue to fall. To achieve this purpose, there are two options in storage technology, a similar GFS, HDFS Sector and other similar cluster file system, and the other is storage area network (SAN) systems based on block device. For example, in IBM's "Blue Cloud" computing platform, the block device interface was provided by the SAN, while HDFS is a distributed file system built over the SAN, and their collaborative relationship were determined by applications in the cloud computing platform.

After the analysis of Google's GFS massive data storage system, we will discuss the popular open source cloud storage system Hadoop's HDFS. Hadoop is an Apache open source organizational design of a distributed computing framework, its core technology HDFS, Map Reduce, H Base were the open source implementation of GFS, Map Reduce, Big table in Google cloud platforms. It is worth mentioning that Hadoop can run on a large number of cheap machinery and equipment. Having many similarities with other distributed file system, the features of HDFS are also very obvious because of its targets and assumptions of Hardware Failure based design, Streaming Data Access, Large Data Sets, Simple Coherency Model, Moving Computation is Cheaper than Moving Data, Portability Across Heterogeneous Hardware and Software Platforms . Although HDFS running on cheap commodity hardware, it can meet the data access requirements of high reliability, high throughput, large data sets responsible for managing the file system namespace, cluster configuration information and stored block copying, storing Metadata of the file system to memory, and this information includes the file information, the file block information for each file, Data Node information of each file Blocks. The Name Node execute file operations, including open, close, rename, catalog maintenance, it also determines the mapping between the Block and Data Node. Internally, a file is divided into one or more Blocks. Data Node is responsible for the read and write requests from Clients, and executing instructions of Block establish, delete, copy and other, issued by the Name Node. Data Node stored Blocks and their Metadata in the local file system, and periodically sending information of existing Blocks to the Name Node at the same time. Clients are applications to get a file from the file system. In the past nearly ten years, the academia and business put forward similar "Cloud computing" concept and mode in succession, such as "Grid Computing", "On demand", "Utility Computing ", " Internet Computing", "Software as a service ", " Platform as a service" and other, in order to achieve the target of make full use of network computing and storage resources, wide range of cooperation and resources sharing, high efficiency and low cost in computing, but the concept of "Cloud computing" formally advanced recently in 2 years. Because of its clear commercial pattern, Cloud computing has become the widespread concern and be generally recognized in both industrial and academic circles, as one of the ten most popular IT technology in 2009. According to IDC, the global market size of Cloud Computing is expected to be increased from 16 billion dollars in 2008 to 42 billion U.S. dollars in 2012, and the proportion of total investment is expected to rise from 4.2% to 8.5%, as shown in the Fig.1. Moreover, according to forecasts, in 2012, the input of Cloud Computing will take up 25% of the annual increase of IT investment, and 30% in 2013.

The network infrastructure services are provided to customers as new commercialized resources, and EC2 has become the current fastest growing business. Google has been dedicated to the promotion of the GFS (Google File System), Map Reduce and Big Table technology-based Application Engine for user's massive data processing. In 2007, IBM launched the "Blue Cloud" computing platform, using the Xen, Power VM virtualization technology and Hadoop technology, in order to help customers build cloud computing environments. Microsoft immediately set out from Live Service to open the market after theannouncement of Windows Azure cloud computing operating system plan,. The first VM ware cloud computing operating system vSphere4 points to the enterprise data center forward, and it transforms enterprise data centers into Cloud Architecture based on virtualization, and so as to help enterprise data center energy to the utility of 30%~50%. As one of the four cloud computing services categories, Sa a S success stories include Sales force CRM (Customer Relationship Management) platform, Ali soft SME management software platform, which also had a great impact. In addition, EMC launched cloud storage architecture, and Apple introduced mobile information services based "Mobile Me" cloud services

Software cost is an important factor when developing a website. It used to be that developers had to buy expensive software (called Integrated Development Environments, or IDEs) in order to build applications. These days, most code can be written using free tools. It can be written using a simple text editor, various free programming text editors and, most commonly, Microsoft’s ubiquitous Visual Studio application, which is available in a free Community Edition for non-corporate use. Companies with more than 5 developers must purchase a license to use Visual Studio, but the cost is competitive with professional IDEs for other platforms. Microsoft also provides Visual Studio Code, a lighter-weight IDE and editor, which is free for everyone, including corporations.

MERITS:

Cost: Purchasing physical storage can be expensive. Without the need for hardware cloud storage is exceptionally cheaper per GB than using external drives.
AccessibilityUsing the cloud for storage gives you access to your files from anywhere that has an internet connection.
RecoveryIn the event of a hard drive failure or other hardware malfunction, you can access your files on the cloud. It acts as a backup solution for your local storage on physical drives.

Syncing and Updating When you are working with cloud storage, every time you make changes to a file it will be synced and updated across all of your devices that you access the cloud from.

SecurityCloud storage providers add additional layers of security to their services. Since there are many people with files stored on the cloud, these providers go to added lengths to make sure your files don't get accessed by someone who shouldn't

DEMERITS:

InternetConnectionCloud based storage is dependent on having an internet connection. If you are on a slow network you may have issues accessing your storage. In the event you find yourself somewhere without internet, you won't be able to access your files.

CostsThere are additional costs for uploading and downloading files from the cloud. These can quickly add up if you are trying to access lots of files often.

HardDrivesCloud storage is supposed to eliminate our dependency on hard drives right? Well some business cloud storage providers require physical hard drives as **well.**

Support for cloud storage isn't the best, especially if you are using a free version of a cloud provider. Many providers refer you to a knowledge base or FAQs.

PrivacyWhen you use a cloud provider, your data is no longer on your physical storage. So who is responsible for making sure that data is secure? That's a gray area that is still being figured out.

IV.FEASIBILITY AND SYSTEM MODULES

4.1 FEASIBILITY STUDY

The feasibility Analysis is an analytical program through project manager determines the project success ratio and through feasibility study project manager able to see either project. The key considerations involved in the feasibility analysis are:

Economic Feasibility
Technical Feasibility
Operational Feasibility
Environmental Feasibility

Economic Feasibility

Hence this project is economically feasible there is no need to involve any cost for this project.

Technical Feasibility

Software Technologies used are PHP and MySql. In the educational institutions, it is possible to update the system in future. No special hardware is required for the purpose of using this system. Hence it is declared that this project is technically feasible.

Operational Feasibility

As the admin work mainly to maintain the Patient and Doctor .Doctor will predict patient cancer disease. Hence it is easy to operate with training. Therefore it is operationally feasible for implementation.

Environmental Feasibility

This project environment is correct as a admin has developed this system and no expenditure is involved under any head and this process is part of admin document management, this project environment is accessible.

4.2 SYSTEM MODULES

System Construction Module

In the first module, we develop the proposed system with the required entities for the evaluation of the proposed model. The data provider (e.g., David) first decides the users (e.g., Alice and Bob) who can share the data. Then, Data Provider encrypts the data under the identities User and uploads the ciphertext of the shared data to the cloud server. When User wants to get the shared data, she or he can download and decrypt the corresponding ciphertext. However, for an unauthorized user and the cloud server, the plaintext of the shared data is not available

Data Provider

In this module, we develop the Data Provider module. The data provider module is developed such that the new users will Signup initially and then Login for authentication. The data provider module provides the option of uploading the file to the Cloud Server. The process of File Uploading to the cloud Server is undergone with Identity-based encryption format. Data Provider will check the progress status of the file upload by him/her. Data Provider provided with the features of Revocation and Ciphertext update the file. Once after completion of the process, the Data Provider logouts the session.

Cloud User

In this module, we develop the Cloud User module. The Cloud user module is developed such that the new users will Signup initially and then Login for authentication. The Cloud user is provided with the option of file search. Then cloud user feature is added up for send the Request to Auditor for the File access. After getting decrypt key from the Auditor, he/she can access to the File. The cloud user is also enabled to download the File. After completion of the process, the user logout the session.

Key Authority (Auditor)

Auditor Will Login on the Auditor’s page. He/she will check the pending requests of any of the above person. After accepting the request from the above person, he/she will generate master key for encrypt and Secret key for decrypt. After the complete process, the Auditor logout the session.

V.TESTING AND IMPLEMENTATION

5.1 TESTING

Implementation is the stage of the project when the theoretical design is turned into a working system. This is the final and important phase in the system life cycle It is actually the process of converting the new system into a operational one

.

Unit Testing

Unit testing comprises the set of tests performed by an individual programmer prior to integration of the unit into a larger system. The module interface is tested to ensure that information properly flows into and out of the program unit. The local data structure is examined to ensure that data stored temporarily maintains its integrity during all steps in algorithm’s execution. Boundary conditions are tested to ensure that the module operates properly at boundaries established to limit or restrict processing. All independent paths through the control structure are tested. All error-handling paths are tested.

Block Box Testing

Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied virtually to every level of software testing: unit, integration, system and acceptance. It is sometimes referred to as specification-based testing.

5.2 SYSTEM IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned into a working system. This is the final and important phase in the system life cycle It is actually the process of converting the new system into a operational one.

VI.CONCLUSION AND FUTURE WORKS

It has been proposed another novel system to remove the single point execution bottleneck and increment the efficiency of the current CP-ABE scheme. By successfully reformulating CP-ABE cryptographic system into this novel structure, the proposed system gives a fine-grained, robust and secure access control with one-CA chosen among multi-AAs for public cloud storage. This plan utilizes various AAs to share the heap of thetedious authenticity check and standby for serving subsequent client demands. It has been proposed an auditing technique to trace the AAs for their potential incorrect behavior. An observer is introduced to monitor CA and if there is any malicious behavior then new CA has chosen among AAs which increases the security. It has been conducted detailed performance and forensic analysis to verify that this scheme is efficient and secure. The security analysis shows that the scheme could effectively resist individual and colluded malicious users, as well as the honest-but-curious cloud server

VII.FUTURE ENHANCEMENT

In our enhanced system, we employ the fact that the secret information loaded into the enclave cannot be extracted. However, recent work shows that enclave may leak some amounts of its secret(s) to a malicious host through the memory access patterns or other related side-channel attacks. The model of transparent enclave execution is hence introduced in. Constructing a dual access control system for cloud data sharing from transparent enclave is an interesting problem. In our future work, we will consider the corresponding solution to the problem.

REFERENCES

[1]Joseph A Akinyele, Christina Garman, Ian Miers, Matthew WPagano, Michael Rushanan, Matthew Green, and Aviel D Rubin. Charm: a framework for rapidly prototyping cryptosystems .Journal of Cryptographic Engineering, 3(2):111–128, 2013.

[2]Ittai Anati, Shay Gueron, Simon Johnson, and Vincent Scarlata.Innovative technology for cpu based attestation and sealing. In Workshop on hardware and architectural support for security and privacy (HASP), volume 13, page 7. ACM New York, NY, USA, 2013.

[3]Alexandros Bakas and Antonis Michalas. Modern family: A revocable hybrid encryption scheme based on attribute-based encryption, symmetric searchable encryption and SGX. InSecureComm2019, pages 472–486, 2019.

[4]Amos Beimel.Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion ,Haifa, Israel, 1996

5]John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In S&P 2007, pages 321–334. IEEE, 2007 .

[6]Victor Costan and Srinivas Devadas. Intel sgx explained. IACR Cryptology e Print Archive, 2016(086):1–118, 2016.

[7]Ben Fisch, Dhinakaran Vinayagamurthy, Dan Boneh, and Sergey Gorbunov. IRON: functional encryption using intel SGX .In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, pages 765–782, 2017.

[8]Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of a symmetric and symmetric encryption schemes. In Advances in Cryptology-CRYPTO 1999, pages 537–554. Springer, 1999.

[9]Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute -based encryption for fine-grained access control of encrypted data. In ACM CCS 2006, pages 89–98. ACM, 2006.

[10] Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, and ManHo Allen Au. Improving privacy and security in decentralized cip hertext-policy attribute-based encryption . IEEE transactions on information forensics and security, 10(3):665–678, 2015.

[11] Christofer Hoff. Cloud computing security: From ddos (distributed denial of service) to edos (economic denial of sustainability).http://www. rationalsurvivability.com/blog/?p=66.

[12] Joseph Idziorek, Mark Tannian, and Doug Jacobson. Attribution of fraudulent resource consumption in the cloud. In IEEE CLOUD2012, pages 99–106. IEEE , 2012.

[13] Simon Johnson, Vinnie Scarlata, Carlos Rozas, Ernie Brickell, and Frank Mckeen. IntelR©software guard extensions: Epid provisioning and attestation services. White Paper, 1:1–10, 2016.

[14] Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, HyesoonKim, and Marcus Peinado. Inferring fine-grained control flow inside sgx enclaves with branch shadowing. In26th USENIX Security Symposium, USENIX Security, pages 16–18, 2017.

[15] Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han. Ksf-oabe: outsourced attribute-based encryption with keyword search function for cloud storage . IEEE Transactions on Services Computing, 10(5):715–725, 2017.

[16] Jiguo Li, Yao Wang, Yichen Zhang, and Jinguang Han.Ful-l verifiability for outsourced decryption in attribute based encryption. IEEE Transactions on Services Computing, DOI:10.1109/TSC.2017.2710190, 2017.

[17] Wei Li, Kaiping Xue, Yingjie Xue, and Jianan Hong.Tmacs: A robust and verifiable threshold multi-authority access control system in public cloud storage. IEEE Transactions on parallel and distributed systems, 27(5):1484–1496, 2016.

[18] Ben Lynn et al. The pairing -based cryptography library . Internet : crypto. stanford. Edu /pbc/[Mar. 27, 2013], 2006.

[19] Frank McKeen, Ilya Alexandrovich, Alex Berenzon, Carlos V.Rozas, Hisham Shafi, Vedvyas Shanbhogue, and Uday R. Sava-gaonkar. Innovative instructions and software model for isolated execution. In HASP@ISCA 2013, page 10, 2013.

[20] Antonis Michalas. The lord of the shares: combining attribute-based encryption and searchable encryption for flexible data sharing. In SAC 2019, pages 146–155, 2019

[21] Jianting Ning, Zhenfu Cao, Xiaolei Dong, Kaitai Liang, Hui Ma,and Lifei Wei. Auditableσ-time outsourced attribute-based encryption for access control in cloud computing. IEEE Transactionson Information Forensics and Security, 13(1):94–105, 2018.

[22] Jianting Ning, Zhenfu Cao, Xiaolei Dong, and Lifei Wei. White-box traceable CP-ABE for cloud storage service: How to catch people leaking their access credentials effectively. IEEE Transactions on Dependable and Secure Computing, 15(5):883–897, 2018.

[23] Jianting Ning, Zhenfu Cao, Xiaolei Dong, Lifei Wei, and XiaodongLin. Large universe ciphertext-policy attribute-based encryption with white-box traceability. In Computer Security-ESORICS 2014,pages 55–72. Springer, 2014.

[24] Jianting Ning, Xiaolei Dong, Zhenfu Cao, and Lifei Wei.Ac-countable authority ciphertext-policy attribute-based encryption with white-box traceability and public auditing in the cloud. In Computer Security–ESORICS 2015, pages 270–289. Springer, 2015.

[25] Jianting Ning, Xiaolei Dong, Zhenfu Cao, Lifei Wei, and XiaodongLin. White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes. IEEE Transactions on Information Forensics and Security, 10(6):1274–1288, 2015.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 ☎ 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details