IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Novel Framework For Security Issues And Data Recovery In Cloud Computing

Ms. R. Rajalakshmi[1] , Dr. S. Mangayarkarasi[2]

[1] Research Scholar, School of Computing Science, Vels Institute of Science, Technology & Advanced Studies, Chennai, India.

[2] Professor, School of Computing Science, Vels Institute of Science, Technology & Advanced Studies, Chennai, India.

Abstract: Due to the growing acceptance of cloud computing, both consumers and businesses are quickly adopting cloud services for a variety of purposes. The primary driver behind this change is the abundance of advantages that cloud services offer, like cheap prices, processing power, and online storage. One of the key ideas when discussing storage devices, which serve as the foundation of the cloud infrastructure, is data recovery. Customers' private or confidential data can be recovered via data recovery techniques by someone who has access to such servers or devices, even after the customers have erased it from the cloud. Users' privacy is compromised and there is a security risk when such data is rebuilt. From the user's perspective, the data has already been removed from the cloud, but they are unaware that somebody else has access to it even after they have gained access. In this research, we investigate the potential security risk associated with users using data recovery tools on cloud servers after they have erased their data. Rename is a straightforward technique that we have suggested be used to solve this issue.

Keywords: Cloud computing, Data recovery, Data security, Security issues, Cloud reconstruction

1. INTRODUCTION

The field of computer science is quickly advancing thanks to advancements in large data processing, cloud computing, access controls, Internet of Things (IoT), and other areas. The ecosystem is changing quickly, which is causing many advancements in data analytics, cloud computing, and other related sectors. The cloud offers several options for supporting diverse services and efficiently managing them. Customers can pay for each use and access a variety of online services, among other benefits. Anyone can use cloud services through public cloud service providers, or consumers and organisations can create their own private cloud to suit their needs [1].

One of the key factors contributing to the cloud services' quick adoption is the variety of benefits they offer to users. On top of established technologies, which comprise hardware and some software programmes, the cloud is being developed or accepted. With such technologies, the cloud is developing on top of them without any additional advancements in platform, software, or infrastructure, save from the requirements that must be created specifically for the cloud. This is one of the factors driving the cloud's quicker evolution for consumer benefit [2].

Due to the cloud's and computing's quick development, a lot of businesses began offering cloud services.Customers now find it more difficult to select the right cloud service providers considering this evolution in order to achieve their objectives. Because it presents numerous security risks for the client to select services (cloud service providers) that are not part of their company. Customers would be inclined to select service providers who offer enhanced security protecting their data in the cloud due to the constant emergence of new threats [3].To meet their data processing needs, some individuals and small businesses began setting up their very own private clouds. While it may be costly for them to run the cloud infrastructure and defend against external threats, these privately owned clouds are most likely not exposed to actual networks; instead, they may be operating on them behind firewalls.

Security is one of the key issues with the cloud that needs to be taken care of. In order to advertise cloud services to potential new users and entice existing ones to stick around, security issues in the cloud must be fixed at every stage. Although cloud service providers are better suited to handle security-related concerns than their clients are, some problems can also be resolved with the aid of outside apps [4]. We have discussed some cloud-related issues in [5] and how homomorphic encryption can be used to address them.One must have a thorough understanding of data recovery, its applicability to cloud systems, and the steps that must be taken to safeguard cloud data after use.

This study examines data recovery in a cloud computing setting. Since data recovery might present security concerns for client data, if customers have erased their data in the cloud, it may still be feasible for someone who has access to the cloud infrastructure to obtain access to their data.The primary contribution of this research is to demonstrate the possibility of data recovery in a cloud context. The potential for cloud-based data recovery raises security concerns that must be resolved to safeguard customers' lost data. In order to address this issue, we have suggested a structure that protects cloud data before it is erased by utilising the straightforward rename module. If the suggested structure is used, client information cannot be recreated without knowledge of the data's true format.

The following is how the rest of the paper is arranged: Section II introduces cloud computing including the security challenges that this paper will address. proceeded to discuss cloud data recovery in Section III, using one application as a resource for data recovery tools. Section IV presents a suggested structure for resolving the issue. The conclusion is drawn in Section V.

2. CLOUD COMPUTING

2.1 What is Cloud Computing?

The utilisation of hosted services, including servers, databases, networking, software, and data storage via the internet, is referred to as cloud computing. A cloud service provider manages the physical servers where the data is kept. In cloud computing, computer system resourcesparticularly data storage and processing powerare made available on-demand and are not directly managed by the user.

A user can save files in the cloud, which allows them to be accessible from any location if they're connected to internet access, rather than on a hard drive or storage device. Infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) are the three main categories into which cloud services can be separated. Public, private, and hybrid clouds can also be categorised according to the deployment model. Moreover, cloud computing can be separated into front-end and back-end levels. The front-end layer is the one that users interact with. Through cloud computing software, a user can access the data stored in the cloud thanks to this layer.

2.2 Types of Cloud Computing

Either the service type or the deployment model can be used to categorise cloud computing. We may categorise cloud computing into three types: public, private, and hybrid cloud, depending on the installation model. In addition, depending on the services the cloud model provides, it can be categorised as platform-as-a-service (PaaS), software-as-a-service (SaaS), or infrastructure-as-a-service (IaaS).

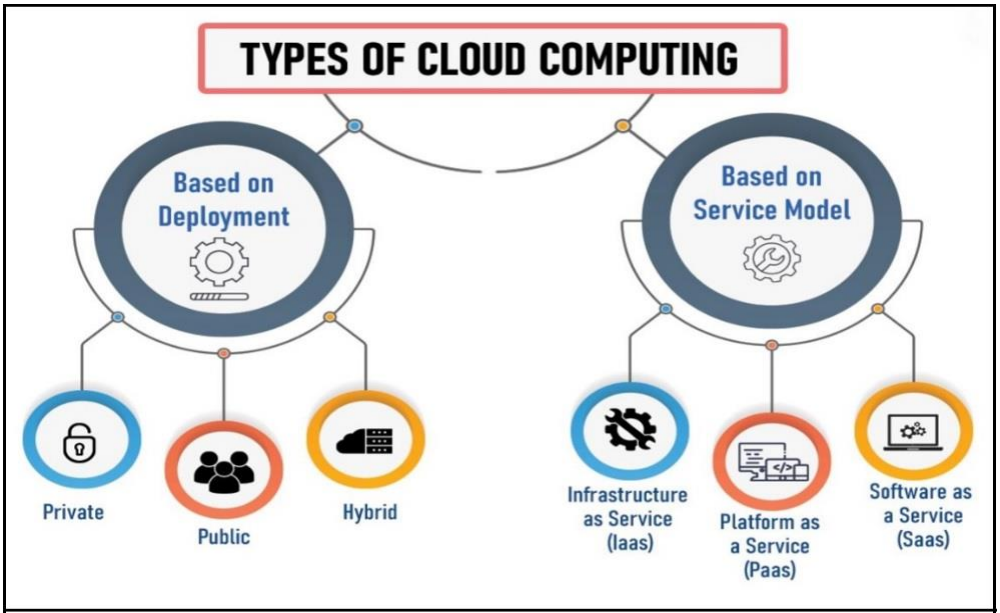

Figure 1: Types of Cloud Computing

Private cloud

In a private cloud, a single organisation has exclusive access to computer services provided across a private IT network. A private cloud, also known as an internal, enterprise, or business cloud, is often controlled by internal resources but is inaccessible to external parties. All the advantages of a public cloud, like flexibility, scalability, and self-service, are also offered by private cloud computing, along with extra protection, control, and customisation.By using internal hosting and business firewalls, private clouds offer an increased level of security to make sure that sensitive data held by an organisation is not accessible by outside parties. The disadvantage of private cloud, nevertheless, is that the company is now in charge of managing and maintaining the data centres, which can need a lot of resources.

Public cloud

In contrast to private clouds, public clouds are made available to anybody who is interested in using or buying them. They can be free or sold on an as-needed basis, meaning users only pay for computing power, space, and bandwidth they use. as the cloud service provider manages the system, public clouds may assist businesses save money on purchasing, managing, and keeping on-premises infrastructure. They also provide scalable RAM and adaptable bandwidth, which makes it easier for organisations to scale their storage requirements.

Hybrid cloud

Public and private cloud functionalities are combined in hybrid cloud computing. As computation and pricing requirements change, workloads can be moved among both public and private clouds using the "best of both worlds" cloud concept. Hybrid cloud computing is useful when processing and computing demand is erratic.To manage the overflow, companies can expand the infrastructure they have on premises to include the public cloud through opens a new window, all the while making sure that their data is protected from access by outside data centres.As opposed to spending money on resources that might not be utilised for an extended amount of time, businesses using a hybrid cloud model simply pay

for the resources that are utilised momentarily. To put it briefly, a hybrid cloud provides all of the advantages of a public cloud minus the security dangers.

Infrastructure as a service (IaaS)

In cloud computing, servers, storage, and networking via a virtual interface are all handled by a service provider under the terms of infrastructure as a service, or IaaS. With this service, the customer has control on the storage, OSes, and installed apps without having to worry about managing the cloud infrastructure. A third-party provider hosts the servers, storage, software, hardware, and other infrastructure elements rather than the user. Additionally, the vendor keeps a backup copy and hosts the user's applications.

Platform as a service (PaaS)

Platform as a Service, also known as PaaS, is a subset of cloud computing that offers a cloud-based development and deployment the environment that saves users the trouble of creating and managing infrastructure. It gives users access to resources for creating cloud-based applications; these resources are paid for on a pay-as-you-go basis by a vendor and are accessible via a secure connection.Users can control the deployed apps with PaaS, but they are not required to manage the foundational infrastructurethat is, the servers, operating systems, network, or storage. This relieves organisations of the burden of managing software upkeep, planning, and resource acquisition, allowing them to concentrate on the implementation and administration of their applications.

Software as a service (SaaS)

Software as a service, or SaaS, enables customers to subscribe to cloud-based software from vendors. Users of this kind of cloud computing don't have to download or install apps on their local device. Rather, the apps are situated on a distant cloud network that may be accessed directly via an API or the internet. All the hardware, middleware, software for applications, and security are managed by the service provider under the SaaS model. SaaS, often known as "hosted software" or "on-demand software," enables businesses to easily optimise their upkeep and support.

3. DATA SECURITY ISSUES IN CLOUD

Undoubtedly, cloud computing offers a multitude of benefits; yet it also presents certain security risks. The security issues with cloud computing are listed below.

Misconfiguration

One well-liked method of saving money and gaining remote access to resources is cloud computing. On the other hand, if the resources in the cloud are set up properly, cloud security risks cannot materialise. The biggest threat to cloud security is misconfiguration since users need to make sure their data and apps are properly protected in the cloud. Users need to make sure that their apps are configured correctly and that their data is safe in order to prevent this security risk. A service for cloud storage that provides security features like encryption or restriction of access can be used to achieve this.Highly sensitive information in the cloud can also be protected by putting security measures in place like password restrictions and authentication. Users can strengthen the security associated with their cloud computing architecture and guard against online attacks by using these measures.

Unauthorized Access

One of the biggest issues with cloud security that companies have is unauthorised access to data. Businesses may store and retrieve data conveniently over the cloud, but this also exposes data to security dangers. Malware attacks, data theft, and unauthorised access to user information are examples of cloud security breaches. Businesses need to make sure that only people with permission may access their data

in order to safeguard it against these kinds of attacks. Encrypting private information in the cloud is another security measure that businesses can use. Assuring that only authorised people can access it will be made easier. Businesses may secure and maintain the integrity of their data by putting security measures like encryption and backup processes in place.

Hijacking of Accounts

One of the most common breaches in cloud security is account hijacking. Utilising cloud-based services and apps raises the possibility of account theft. To keep safe on the cloud, users must be watchful about safeguarding their passwords as well as other private information. Strong passwords, safety concerns, and two-factor authentication are ways that users can safeguard themselves when logging into their accounts. In addition, they can keep an eye on the activities associated with their accounts and take precautions against unwanted access or use. By doing this, you can make sure that hackers are unable to access their private information or take over their accounts. In general, maintaining security awareness and upgrading your security protocols are essential to cloud computing security.

Lack of Visibility

Businesses may now access and keep their data online more easily thanks to cloud computing, but there are risks involved. Consequently, businesses must safeguard their data against theft and unwanted access. However, because cloud computing relies on distant computers, it also presents security risks. Businesses need to use security methods such robust authorization, data loss prevention (DLP), data breach recognition, and data breach response to make sure that only authorised sources may access their systems.Visibility is key when it comes to cloud computing, and companies need to evaluate security processes and procedures on a regular basis to find weaknesses and threats when they become serious issues. Through the implementation of security best practices and essential measures, organisations may guarantee the protection of their data in a cloud-based environment.

Data Privacy/Confidentiality

Concerning cloud computing, data security and privacy are crucial challenges. Businesses may utilise their data via cloud computing from any location in the world, this presents security issues. Businesses must make sure that only authorised users can access their data because they have no control over who else can access it. Hackers that manage to obtain access to corporate data may commit data breaches. Due to the growth of big data and the expanding usage of cloud computing in business, there will be even more concerns regarding the security and privacy of data in the upcoming years.

External Sharing of Data

One of the biggest issues with cloud security that companies have is external data sharing. Whenever data is shared with outside vendors who the company must first screen and approve, problems can occur. External data sharing may also result in theft, fraud, and the loss of important corporate data. Businesses need to have strong security measures in place, such encryption, as well as data management procedures, to stop these threats. Furthermore, it will support maintaining the confidentiality and security of sensitive data. Businesses may guarantee the dependability and integrity of their data and prevent unwanted access by putting in place the necessary security measures. All things considered; external data sharing poses a serious threat to cloud security that companies need to overcome to remain competitive.

Legal and Regulatory Compliance

A cloud is a potent instrument that can lower expenses and boost operational effectiveness for businesses. Cloud computing, however, brings additional security issues that need to be resolved to safeguard data and guarantee adherence to legal and regulatory obligations. To guarantee the security and integrity of all their cloud-based systems, organisations need to make sure that data is protected and that

they adhere to all applicable laws and regulations. Organisations that use cloud computing encounter a few issues, including malware, data breaches, and phishing.

It's critical to conduct regular security audits, keep security configurations current, adopt strong authentication procedures, employ multi-factor authentication where necessary, and upgrade operating systems and software on a regular basis in order to counter these cyber security risks. Although cloud computing can make intrusions more likely, companies who are vigilant about their safety measures can remain one step ahead of their rivals in this quickly evolving market.

Unsecure Third-party Resources

The websites, apps, and services that are not within the cloud provider's control are referred to as third-party resources. It's possible that some resources have security flaws, making it possible for unauthorised parties to access your data. In addition, hackers could be able to access your data stored in the cloud using unprotected third-party resources. These flaws could jeopardise your security. As a result, it is crucial to guarantee that cloud computing uses only reliable and secure resources. Furthermore, it will lessen the possibility of unauthorised data loss or breach and assist guarantee that only authorised persons have access to data.

Cyber security risks might arise from using unsecured third-party resources, particularly when working with private information stored in cloud storage accounts. These resources provide hackers with the ability to access your cloud data and infrastructure. Strong security measures like multi-factor authentication and stringent password regulations can be put in place to assist reduce this danger. Furthermore, you may guarantee that only authorised users have access to data and lower the possibility of unauthorised data loss or breach by limiting access to only reliable resources.

4. DATA RECOVERY IN CLOUD

The alternatives for data recovery in the cloud that are practical and accessible will be covered in this section. Data recovery tools operate using carving techniques or related memory analysis. Numerous open-source programmes and businesses offer these services for data recovery [8]. We won't go into great depth about each method, but we will give you an overview of one tool that can be utilised to recover files that were deleted in a cloud setting.

- **PhotoRec:** One tool that users can use to recover data from memory devices after it has been erased is called PhotoRec. It is accessible for free. Reading memory blocks and recreating the data stored in the respective memory locations is how the application operates. An open-source programme called PhotoRec uses a different file system. This programme can retrieve about 480 different kinds of data. Blocks of files are stored in most current file formats. Typically, contiguous memory blocks are used to hold these linked data blocks. When these documents are removed, the memory associated with that data is often designated as empty space and made available for allocation, along with any associated metadata. Deleted data will still exist in these memory regions once new data is added, but it won't be visible to our systems. With data recovery programmes like PhotoRec, the erased data can be recovered. PhotoRec begins data recovery by comparing the content of the data with the right format of the data, using the initialization record of these devices to determine the block size [9].
- **Yelp Photo Dataset:** We utilised the Yelp Photo Dataset 11 [10] for data reconstruction. This Yelp photo dataset comprises over 200,000 JPEG pictures of different foods. The dataset has a total size of 7.50 gigabytes (GB). These photos were primarily used to test the amount of content that could be recovered after deletion utilising memory analysis methods. The primary purpose of utilising this dataset is to determine how much data can be recovered and because it contains no confidential information.

- **Results:** Yelp Photo Dataset 11, which included 200,000 JPEG photos, has been removed. After that, we recovered the data using the data recovery tool (PhotoRec). We only lost 2.93 percent of the data because we were capable of to retrieve about 7.28 GB of it.
- **Security Issue:** The results above make it clear that, even after data has been erased from the cloud, it is still feasible to retrieve it using memory analysis methods. If these repair instruments are utilised in Confidential user data that is erased from the cloud can be recovered by the cloud, which has access to the real infrastructure after data is wiped without the customer's awareness. Without the consumers' knowledge, data reconstruction raises privacy and security issues for them.

5. METHODLOGY

The utilisation of cloud services is growing at a quicker rate due to the quick rise in the acceptance of these services to meet organisational or personal goals. Following their completion of using cloud services, customers will gather any analysis or data stored in the cloud and go. However, by jeopardising the private information, data recovery methods akin to those described in the preceding section can be employed to retrieve the data. That provide a straightforward framework in the cloud that helps to address data recovery issues and make it difficult for unauthorised recovery of private customer data post deletion to secure customer data stored in the cloud and address security concerns related to data recovery.

5.1 Elements

Let's start by introducing the various framework components, as depicted in Figure 1, to help you better comprehend the suggested framework.

Customers, also known as users, are the individuals or businesses that use cloud services offered by cloud service providers to accomplish their objectives. The cloud services are theirs to utilise for whatever reason.

The services that service providers offer for users to use across a network are referred to as "cloud" in this sense. Processing power, storage, and other services are examples of cloud services. However, the network is used to deliver each and every service.

The real hardware or infrastructure that consumers employ for storing and processing their data is called a server. A single server may be shared in real time by multiple users.

Rename is a suggested new module that has to be created or might just be a straightforward user-accessible programme for data protection. This rename module's primary job is to retrieve the path or location of the files that need to be removed from the cloud. To make data recovery more difficult, it will change the extensions of all those files to some other file type.

5.2 Methods

Everyone are suggesting the deployment of a new module in this new method in order to protect client data stored in the cloud (rename).Every file will have its name changed, and all file formats will be altered, thanks to the Rename module. Protecting the data is the primary goal of this file format change. Because it is impossible to grasp the data in a different format and makes it difficult for someone else to determine what kind of file the initial data had. The following steps are part of the suggested system:

- The path to the files that users wish to protect must be known to them and passed to the rename module.
- Next, mandate that all files in the cloud have their names changed to reflect a different type of data.

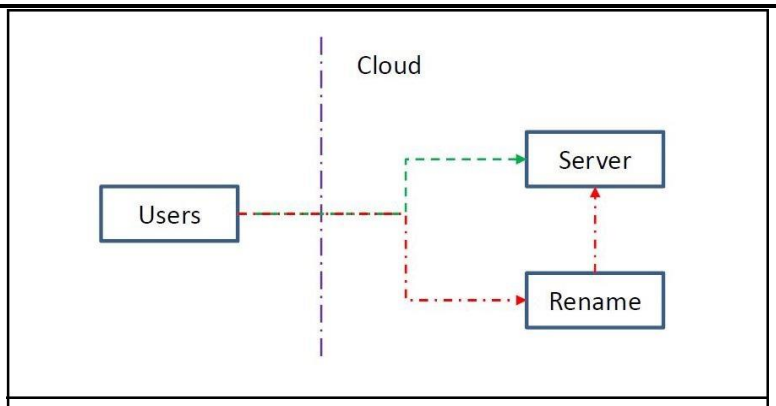

Figure 1: Overview of proposed framework

By using this method, the content isn't really removed, but it prevents anyone from understanding the information included in the data unless they are aware of its precise nature. Users are then free to remove the files or data from the cloud. In this manner, even if someone manages to have access to the infrastructure, they won't be able to comprehend the content even if they might be capable to reconstruct some files using the data recovery techniques discussed in section IV.

A new module (rename) for altering file extensions in comparison to standard cloud architecture makes up the suggested framework. As seen in Figure 1, users will send a request to the Rename module in order to shield the data from reconstruction. Subsequently, the module will begin renaming the files using alternate extensions. The customer can view the updated files with alterations and a few random kinds of data after the renaming process is complete.Customers can then remove the data from the cloud without having to worry about data recovery. Figure 2 displays the sequence diagram after renaming the data.

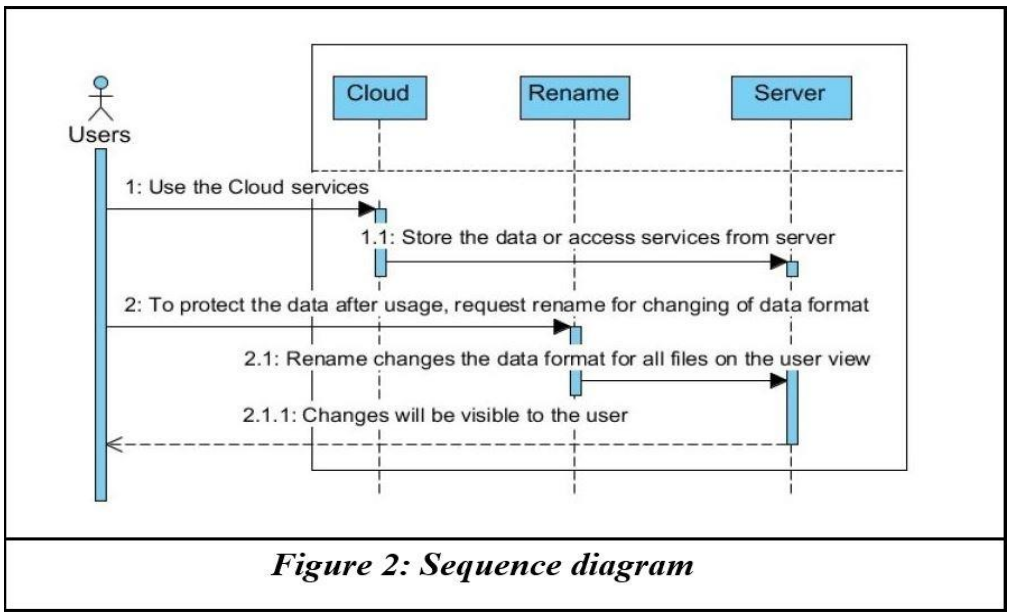

Figure 2: Sequence diagram

5.3 Implementation specifications

To properly safeguard data without compromising on various data formats, the renaming module's implementation requires a thorough understanding of the various forms of data that exist. The kind and format of the data must be determined in the first module. In order to prevent anyone from reconstructing the data into a format that is legible or comprehensible by humans, the module must then identify a different format in which the data must be updated or changed. After the renaming is complete, users won't have to worry about data recovery when they remove the data.

The suggested framework involves multiple stages to secure user data in the cloud. Based on the suggested structure, these steps can be separated into the following steps:After deciding to safeguard the data, the user must call the Rename module and provide the path to the files that require protection.The Rename module will compel the renaming of every one of the files in the specified path to a different format that does not match the original format based on the file type of these files. Even if someone has recreated these files, it will be difficult after the rename operation is complete. Without converting the files back to their original format, it would have been impossible to determine what information was contained in them because the data was in the incorrect format.

5.4 Execution Time

Let's see how long it will take to accomplish the task for renaming the data in a cloud environment using the suggested way. Any type of file containing any kind of data must be renamed to a different type in order to secure the data. Therefore, if we believe that renaming a file in the Cloud will take an identical amount of time (T_{rename})regardless of the format, the time it takes is:

$$T1 = T_{rename}$$

where T1 is the total time needed to rename a single file and T_{rename} represents the time needed to name and rename each file.All of the files must have their names changed in order to safeguard the entire dataset.

$$T_{total} = N * T_{rename}$$

where T_{total} is the total amount of time needed to rename all the content, and N is the total amount of files that need to be renamed in order to protect customer data on the cloud. Equations 1 and 2 make it evident that the time needed for renaming is directly correlated with the quantity of files that need to be renamed. This indicates the additional cost that the customer will incur after utilising the cloud services.

6. CONCLUSION

In this paper, that we have suggested a straightforward architecture for safeguarding client data in cloud environments once users have finished utilising it. The file format notion is how the suggested framework functions. Until these files are changed back to their proper data forms, it will be difficult to interpret the contents of the files in the incorrect data format.We have spoken about our strategy and the several stages we took to complete the suggested framework. In subsequent research, we want to examine the suitability of the suggested framework in real-time situations.

REFERENCES

[1] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, “On technicalsecurity issues in cloud computing”, IEEE International Conference onCloud Computing, pp. 109–116, 2009.
[2] B. P. Rimal, E. Choi, and I. Lumb, “A taxonomy and survey of cloudcomputing systems”, NCM, vol. 9, pp. 44–51, 2009.
[3] S. Paquette, P. T. Jaeger, and S. C. Wilson, “Identifying the security risksassociated with governmental use of cloud computing”, Governmentinformation quarterly, vol. 27, no. 3, pp. 245–253, 2010.
[4] A. A. Nyre and M. G. Jaatun, “A probabilistic approach to informationcontrol”, Internet Technology Journal, ol. 11, no. 3, pp. 407–416, 2010.
[5] J. Surbiryala, C. Li, and C. Rong, “A framework for improving securityin cloud computing”, 2nd IEEE International Conference on CloudComputing and Big Data Analysis (ICCCBDA 2017),2017.
[6] P. Mell, T. Grance, et al., “The NIST definition of cloud computing,”2011.
[7] K. Hamlen, M. Kantarcioglu, L. Khan, and B. Thuraisingham, “Securityissues for cloud computing”, Optimizing Information Security andAdvancing Privacy Assurance: New Technologies: New Technologies,vol. 150, 2012.

[8] F. wiki, “Tools:Data Recovery”, http://www.forensicswiki.org/wiki/Tools:Data Recovery. [Online; accessed 31-Jan-2018].
[9] C. Grenier, “Photorec,” URL http://www.cgsecurity.org/wiki/PhotoRec,2011.
[10] Yelp, “Yelp photo dataset.” https://www.yelp.com/dataset/challenge. [Online; accessed 31-Jan-2018].
[11] Wu Weiqiang, “Comprehensive and multi-angle information securitytechnology research and practice under cloud computing and big dataenvironment”, Communication World, vol. 000(014), pp. 45-46, 2017.
[12] Kong Lingtao, Zhao Hui.,“Data security analysis under the big data cloud computing environment,” Network Security Technology and Application, vol. 000(009), pp. 82-82, 2017.
[13] Zhang Sen,“Research on Data Security in Big Data Cloud Computing Environment”, Information System Engineering,vol. (10), 2017.
[14] Zhang Qian, Yang Huibi.,“Exploration of big data security and privacy protection under cloud computing”, Science Popular (Science Education), vol. 000(010), pp. 192-192, 2017.
[15] Yuan Huihua,“Research on Data Security in Big Data Cloud Computing Environment”, Information Technology and Informatization, 2019.
[16] Sonali Chandel, Tian-Yi Ni, Geng Yang, "Enterprise Cloud: its Growth & Security Challenges in China", 5th IEEE International Conference on Cyber Security and Cloud Computing, 2018.
[17] Nitin Chauhan, Laxmi Ahuja, Sunil Kumar Khatri, "Secure Data in Cloud Computing Using Face Detection: and Fingerprint”, International Conference on Inventive Research in Computing Applications, 2018.
[18] Xiaotong Sun, "Critical Security Issues in Cloud Computing A Survey" 4th IEEE International Conference on Big Data Security on Cloud, 2018.
[19] Hussam Hourani, Mohammad Abdallah,“Cloud Computing: Legal and Security Issues" 8th International Conference on Computer Science and Information Technology (CSIT), 2018.
[20] Naresh,“Data Storage Security Issues in Cloud Computing”, 2nd International Conference on Intelligent Computing”, Communication & Convergence Elsevier Procedia Computer Science, vol. 92, pp. 128-135, 2016.
[21] Wei Nie, Xiangfei Xiao, Zhaohui Wu, Yuanhui Wu, Fang Shen, Xionglan Luo, "The Research of Information Security for The Education Cloud Platform Based on AppScan Technology", 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud), 2018.
[22] Ruixuan La, Chenglin Shen, Heng He, Ruixuan Li, Chenglin Shen, Heng He, Zhiyong Xu, and Cheng-Zhong Xu, "A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing”, IEEE Transactions on Cloud Computing.
[23] Hongbing Cheng, Chunming Rong, ManyunQian, and Weihong Wang, "Accountable Privacy-Preserving Mechanism For Cloud Computing Based On Identity-Based Encryption", IEEE, 2018.
[24] SambitNayak, Nanjangud C Narendra, Anshu JamesKempf, IEEE 11th International Conference on Cloud Computing. Saranyu: Using Smart Contracts and Blockchain for Cloud Tenant Management, 2018.
[25] Stephen S Kirkman and Richard Newman, “A Cloud Data Movement Policy Architecture Based on Smart Contracts and the Ethereum Blockchain”, IEEE International Conference on Cloud Engineering, 2018.
[26] Stephen S Kirkman, “A Data Movement Policy Framework for Improving Trust in the Cloud Using Smart Contracts and Blockchains”, IEEE International Conference, 2018.
[27] YindongChen, LipingLi, ZiranChen ,"An Approach to Verifying Data Integrity for Cloud Storage", IEEE, 2017.
[28] S.Rajeswari, R.Kalaiselvi, Proceedings of 2017 IEEE International Conference on Circuits and Systems (ICCS 2017), Survey of data and storage security in cloud computing
[29] Shivarajkumar Hiremath, Sanjeev Kunte, " A Novel Data Auditing Approach to Achieve Data Privacy and Data Integrity in Cloud Computing", International Conference ou Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT), 2017.
[30] Akshay Arora, Abhirup Khanna, Anmol Rastogi, Amit Agarwal, "Cloud Security Ecosystem for Data Security and Privacy", IEEE, 2017.
[31] Zhang, Jia Yu, RongHao, Cong Wang, Senior Member, IEEE and KuiRen, Fellow, IEEE, "Enabling Efficient User Revocation in Identity-based Cloud Storage Auditing for Shared Big Data", IEEE, 2017.

[32] Weiwei Kong, Yang Lei, Jing Ma,"Data Security andPrivacy Information Challenges in Cloud Computing", International Conference on Intelligent Networking andCollaborative Systems, IEEE, 2017.
[33] WgCdr Nimi tKaura, LiCol Abhishek Lal, "Survey paper on cloud computing security", IEEE, 2017.
[34] Yong Yu, Man Ho Au. Member, IEEE, Giuseppe Ateniese. Xinyi Huang. Willy Susilo, Yuanshun Dai, and Geyong Min, "Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage", IEEE, 2017.
[35] Jia Yu, Huaqun Wang, "Strong Key Exposure Resilient Auditing for Secure Cloud Storage", IEEE, 2016.
[36] KamileNurSeviş, Ensar Şeker, "Survey on Data Integrity in Cloud", IEEE 3rd International Conference on Cyber Security and Cloud Computing, 2016.
[37] Jia Yu, Kuilken, Senior Member, IEEE, and Cong Wang Member, IEEE, "Enabling Cloud Storage Auditing with Verifiable Outsourcing of Key Updates", 2015.
[38] Tunisha Saxenal, Vaishali Chourey, A Survey Paper on Cloud SecurityIssues and Challenges.
[39] Durga Priya G, Soma Prathibha." Assuring Correctness for Securing Outsourced Data Repository in Cloud Environment", IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), 2014.
[40] Vijayalakshmi, R., Prathibha, S.,"A novel approach for task scheduling in cloud", Fourth International Conference on Computing. Communications and Networking Technologies (ICCCNT), 2013.
[41] Ni Zhang. Di Liu, Yunyong Zhang, "A Research on Cloud Computing Security", International Conference on Information Technology and Applications, 2013.
[42] Mell P. and Granc G., "The NIST Definition of Cloud Computing (Draft)", National Institute of Standards and Technology, Gaithersburg, pp. 6, 2011.
[43] D Carrell., "A Strategy for Deploying Secure Cloud-Based Natural Language Processing Systems for Applied Research Involving Clinical Text", 44th Hawaii International Conference on System Sciences, 2011.