Emperor Journal of Applied Scientific Research

ISSN: 2581-964X **Mayas Publication®** **www.mayas.info**

Volume- VII **Issue- V** **May 2025**

A Framework Design to Backup and Recover the Cloud Computing Data

Dr. A.Priya
Assistant Professor & Head,
PG Department of Computer Science,
Government Arts and Science College,
Tirupattur- 635901

Abstract

Electronic data has been created today in large quantities requiring data recovery services organization's work may experience the various type of disasters whether it was natural or man-made, which may result in huge loss of data. In an experimental evaluation, the encryption and spatial scrambling performance and the average response time have been estimated in terms of the data file size. The Data user verifies the document with the proof and decrypts the encrypted file if verification is correct. Finally, it describes a prototype system configuration for several practical network applications, including the hybrid utilization of cloud computing facilities and environments which are already commercialized.

Keywords: Cloud Computing, Data Backup, Data Recovery.

I. INTRODUCTION

Cloud computing is a distributed community that provides calculating or storage space as services to end users. The architecture/model of cloud computing is that all servers, networks, presentations or other basics connected to the facts center are accessible to the end users. Cloud computing is upward in attention of technology and business organizations, but this is useful for solving social problems. It can also be beneficial. Cloud computing refers to online operation, configuration or access to applications. It provides online data storage, infrastructure or submissions.

Cloud computing allows individuals and businesses to shift the burden by managing large amounts of data or performance processes that require computing for powerful servers.

Due to the growing approval of cloud figuring, more or more data proprietors are being encouraged to subcontract their data to cloud attendants in order to provide great convenience and reduce data management costs.

Data tenants provide services to many businesses and companies, and they insist on improving data security standards by following a covered method, including following: data encryption, key organization, strong admission controls, or security intellect.Today the demand of Cloud computing is increased rapidly as it offers dynamic flexible scalable resource allocation.

Cloud computing provide computing resources as a reliable service such as IaaS, PaaSand SaaS to users as pay as you go manner[1]. The Cloud provider can gain profit only if it provides services under the terms and condition stipulated between provider and customer mentioned in SLA. Also, by efficient management of data enter; Cloud providers can reduce the cost of maintaining the servers and provide their services at lower cost and make more revenue.

The main expenditure has been noticed due to the power consumption by data enter. It has also been noticed, the life of hardware is reduced if they work in high temperature continuously. The data enter emits huge amount of harmful CO2gas and tremendous heat. So, for the servers to be work reliable require their energy efficient and ecofriendly maintenance. Many methods have been proposed to solve the power consumption problem and task scheduling problem in Cloud.

In Cloud computing, each application runs on a virtual machine, where the resources be distributed virtually. hosting and management surroundings for submission services. Therefore, the task scheduling problem in Cloud is two step problems [2,3].Thus, there is a requirement, when proposing an approach of solving one issue at one level; must also consider the other related issues either same level or an other level i.e. some kind of integrated task scheduling approach need to be proposed.

Related Work

Here it is discussed that, cloud computing originates with many potentials or contests at the same time. If the security is consistent and secure, the load or compensation provided by cloud computing will give us less sureness [4]. Sometimes, a person desires to store 35 files on a isolated cloud server. If you do not know exact location of the data storage, it may violate and may affect data security behaviour in some areas. The security of data or its position is an imperative aspect of computer sanctuary.

Transferring complex data to the cloud server, relocating statistics from cloud to client computer, or storing client's personal data on the server are three situations or complex situations in cloud computing Specific environmental considerations. Confidence in the home can become the key to construction a effective cloud computing situation.

Such threats contain abortion, harassment, mugging, moderation or comparable attacks. With this DDoS attack (denial of service), it is a common but major persecution of cloud infrastructure.

To improve the security of cloud computing, many efforts have been made, especially for the cloud for the public, it is still unsettled. This paper comprises9 major threats to cloud security and censorship that have been publicised by Cloud Security Alliance (CSA), such as data quarrying, data loss, clarifications or traffic operation, containing session management, SQL injection, web-based web design, execution, and packages.

Attacks, malware attacks, social engineering doses, phishing doses, unsolicited transportations and APIs, Denial of service, malicious miners, exploitation of cloud services, inadequate readiness and delivery of technical susceptibilities [5,6]. Here it offers decoy technology based on user behaviour examination as a solution to identify doses of cloud theft in order to perceive invalid users and prevent their users from being hacked to be eradicated.

The decoy file will immediately confuse or confuse the attackers so that they do not know what is real or what is not, or they are designed to create an alarm even if the aggressor catches them. The decoy file contains the Key Hash Message Authentication Code (HMAC), which is concealed in title section of file. The authors conclude that with the growth of cloud-based architecture, future will face security and secrecy dares, and future implementation systems will be needed.

Here the position of Kerberos authentication mechanics or requirement to move to multi-cloud. These are necessary measures to ensure cloud security, reliability, transparency and scalability. Kerberos authentication discussions use the authentication server(AS) to verify user/customer authentication by thorough username or password on site, and provide access to the ticket server (TGS) [7]. A customer requesting a service from a cloud provider uses the ticket received from the verification server to request a service ticket from TGS.

This paper also focuses on there inforcement method and the Kerberos method used to migrate to multiple clouds. In this article, Cloud supports individuals or small industries to better design and build business-level services. However, there is still widespread concern among large companies to transfer control of data to cloud providers. Users must be content that they can defend discretion ,integrity or admission to data complete controls and regulations.

There are several security issues in the cloud business, but these are divided into two:; The second is safety subjects facing customers [8].For example, verification and safety checks. Here it introduces security verification models, security threats to the user interface and vulnerabilities. Cloud computing security architecture has been released, which has security information per computer information, DMZ security for each vApp, system management, image resource management, network information per network, data security.

Strengthening security, licensing and monitoring, and individuality supervision can be enhanced by applying security technology in this cloud-based construction. Patrons provide great critical service. Because cloud services are transmitted over Internet complete traditional system protocols and formats, hidden loopholes of these procedures or threats stood by the redesign have caused many problems or privacy concerns [9,10].

This piece also converses influence of cloud adoption, vulnerability or attack, or defines solution explanations desirable to improve cloud security and privacy. Cloud computing is an innovative new concept that brings many benefits to users. But it can also cause safety problems, which can reduce its use. Understanding vulnerabilities through cloud computing will help organizations move towards the cloud. Because cloud calculating uses many technologies, it also inherits security issues.

In addition, another challenge is the availability of dissimilar types of virtualism technologies, and different types of technologies can handle the process in different ways. Virtual networks are chief goal of some attacks, particularly when related to isolated virtual technologies. They talked about cloud security, and there is no difference between vulnerability and threat.

Here it considers that cloud computing is a normal development of computers and information centers with automated organization systems, product harmonizing, or virtual knowledge. From network- level pressures to application-level threats, cloud is acceptable for many security threats. To maintain cloud security, these security threats need to be controlled [11]. In addition, cloud-based data is defence less to many threats and many other matters, such as security problems, accessibility, confidentiality, and data integrity.

Service workers and customers should ensure that cloud is well protected from any external threats. As a result, there will be a strong or mutual understanding among customer or cloud service benefactor which will minimized customers involvement to minimum, enabling smooth functioning. It also emphasized security matters, privacy or control problems, availability issues, discretion, and honour of data for Cloud Computing and also discussed recent explanations for these security risks. they made a list of security items that all users must be conscious of before selecting to use cloud based facilities and discussed devices for agreeing the user to select precise security stage [12,13].

In the paper contends that, Cloud-based substructure or cloud-related services make up the cost, but the service relies heavily on virtual reality, which is called hypervisor or hypervisor. However, it can also result in safety breaches or privacy subjects. CSA- level security threats provide various levels, such as simulated pressures, such as Do-and-DDo Sshut down services, cloud suspension technology, data loss or leakage, risk factors unknown, abuse, accounting and writing services.

Here the converse common trends of cloud totaling technology, which introduce new risks to existing risks. The main hurdle for organizations setting up cloud services is the risk of service interruption due to attacks such as DoS attacks, information theft, loss of privacy and information corruption [14].

This paper also examines the rarities in the cloud and security threats founded on the concept of attacking cloud creation birds and outlines the security objectives to be achieved. Great cloud computing is another difficult that will be successful in the near future. The benefits of cloud computing are discussed in the paper, but bring more problems, such as virtualization security, application security, self- management, monitoring and validation.

Proposed Work

Data users get every result, proof or public confirmation key, o they or others can even verify freshness, validity and integrity of search results without decryption.

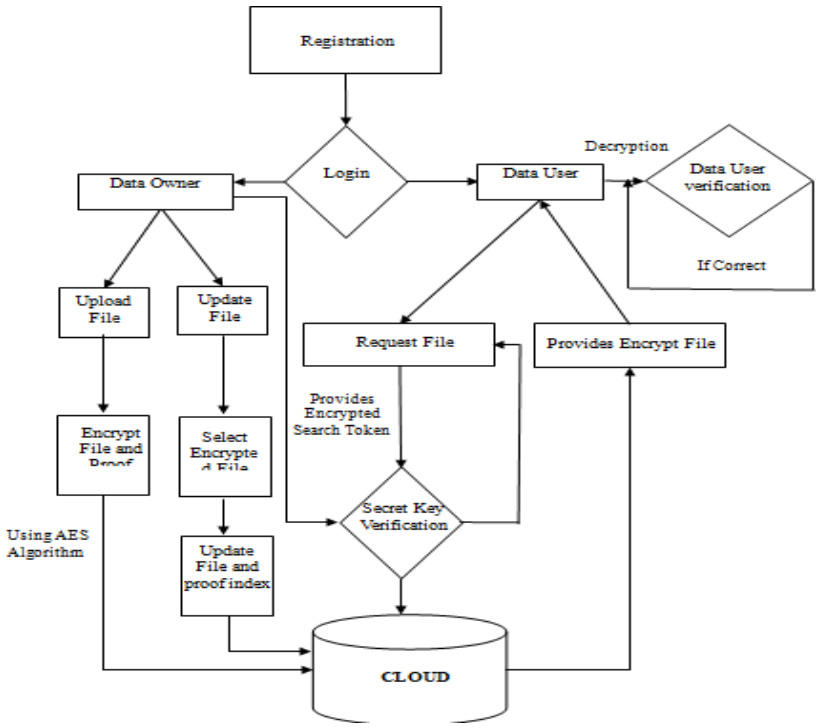


Fig.1: Data flow Diagram

The advantages of cloudity parity services provide a secure return on investment, but the disadvantages are far greater. Compared to traditional computer technology, cloud computing offers various advantages [15]. Cloud computing provides its customers with supercomputing capabilities and high-end devices at affordable prices.

Result Analysis

Many programming languages with language- specific APIs have libraries to open MySQL databases. These include MySQL Connector / Net (the most common languages are C # and VB) used in Microsoft Visual Studio and Java JDBC drivers. An ODBC interface called Modoc allows other programming languages that support ODBC content tocommunicatewithMySQL,suchasASPorColdFusion.MySQLserverorofficiallibraryisimple mented in ANSI C / ANSI C ++.

Modules Description:-

Registration: This is the process of registering or registering to cloud. To take benefit of cloud documents, all data owners and data users must register. During this process, your basic information (such as email, contacts, etc.) will be collected and stored in the cloud. During the registration process, a particular user's cloud ID is generated automatically.

Cloud ID: Each user must produce a Cloud ID or use it to classify an identifier with near security. The identifier does not repeat the identifiers that have been or will be twisted to identify other identifiers. Therefore, the information marked with Cloud ID by liberated parties can later be collective into a single folder or transmitted on same channel without the need to tenacity struggles among identifiers

Data Owner: Data Owner extracts keywords of each article or also figures a keyword Index. Data Owner encrypts documents are keyword Index using a key and outsources in Cloud. Data Owner provides the Public Verification Key and Proof Index to the Data User via Cloud for document verification. Data Owner is the only authorized person to add, modify, or delete the document(s) from the cloud.

Cloud Service Provider: The cloud service provider can see all uploaded or transferred documents in cloud. CSP obtains document request from the data user, verifies identity before granting permission, and then CSP executes query or revenues encrypted document based on search token, or also returns document with other evidence on document to confirm search results.

Public Verification Key: Public verification key is a safety quantity planned to make sure that your document outsourced in cloud doesn't get hacked. By confirming public key, the Data Owner and the Data Use radding added coverof defense to documents or files in the cloud by authorizing each other's identities

Data User: Data User sends a appeal to the cloud server. After request granted from the Cloud, the Data User receiving the Public Verification Key from the Cloud generated by Data Owner. The Data User now decrypts and downloads the encrypted documents, after verifying with the Public Verification Key. After receiving verification from cloud, the data user will download the file within a particular time limit.

Fig2: DataOwner Login.

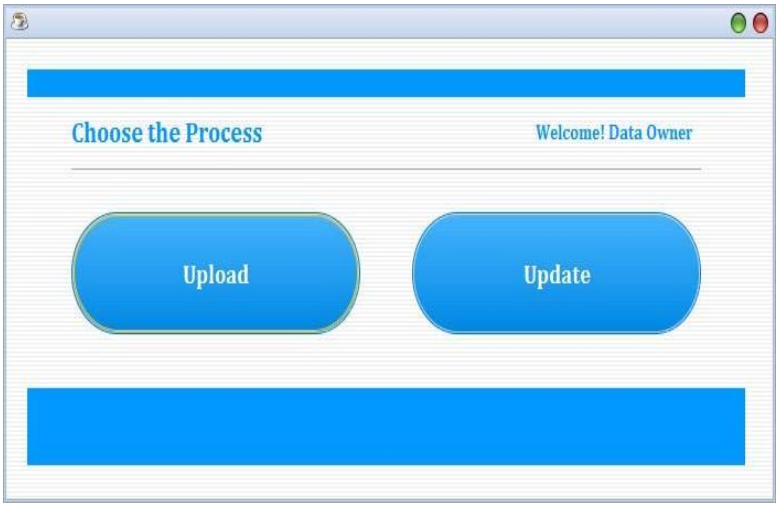


Fig3: DataOwnerFileupload/update screen.

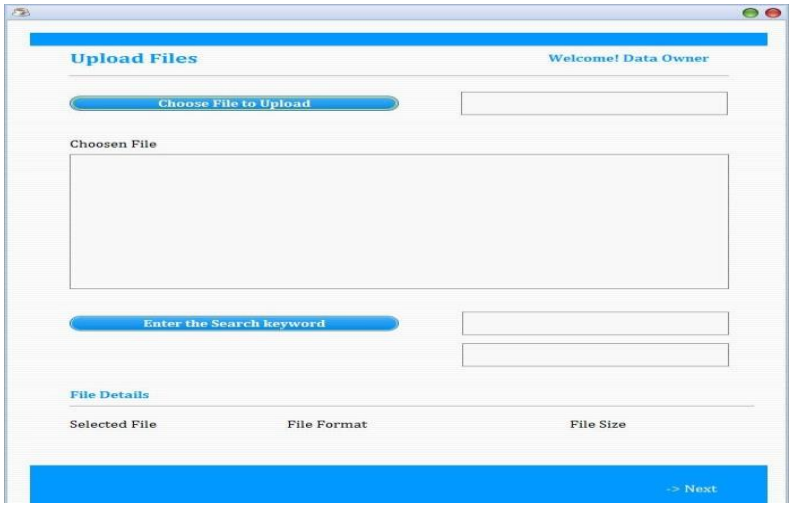
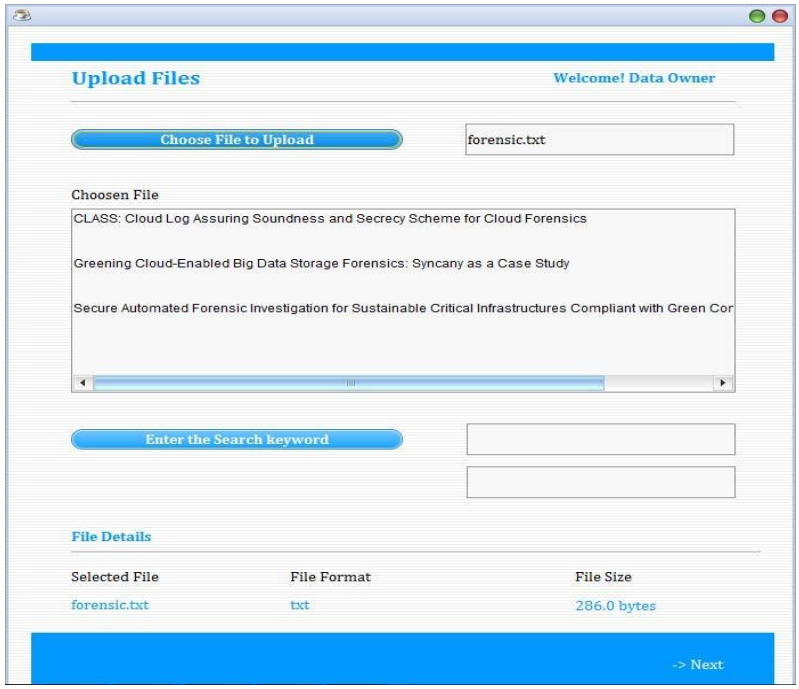
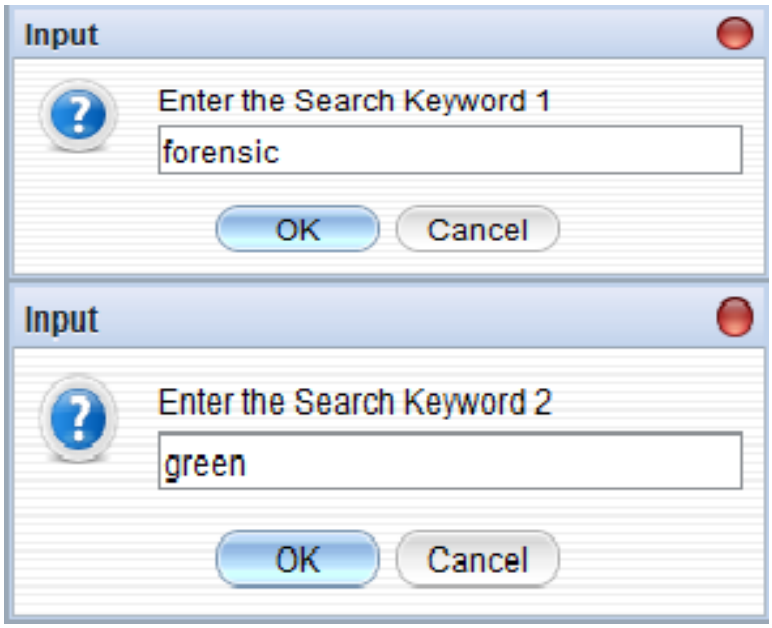


Fig4: Screen after uploading file by data Owner.





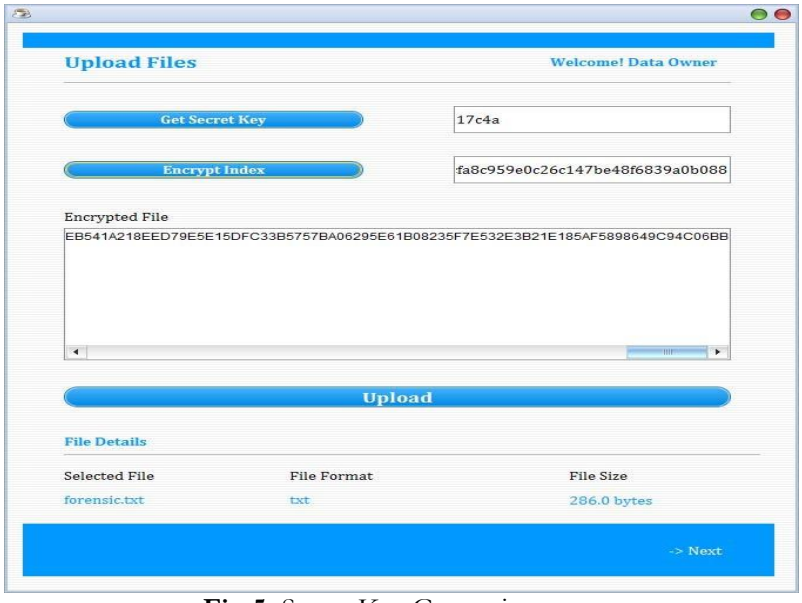


Fig 5: Secret Key Generation.

II. CONCLUSION

In implementation there are many models Collected on the web servers. It helps in reducing allocation of geographical area required for storing records and also promotes paperless work. Time consumed for searching required documents is less. Every organization prefers computerization as well as remotely accessible web services. Hence data security and protection come in highest priority so recent developments will be on securing and protecting data collection on web server.

It is focused on privacy, security and access to the cloud computing environment. While cloud security services can be well-designed and succeeded by experts, they can provide effective organization or threat valuation services. Though, threats it was discussing here to show that the implementation of present security mechanisms in the cloud should be carefully considered.

In order to accelerate the development of cloud computing, many improvements to existing mechanics are needed, and new innovation systems need to be established. we plan to cover the planned work to other parts of cloud. Cloud computing brings various tasks for structure or submission developers, engineers, system administrators and service providers. we will discuss some of the tasks associated to security or privacy managing in cloud.

III. REFERENCES

[1] Vahid Ashktorab and Seyed Reza Taghizadeh, Security Threats and Countermeasuresin Cloud Computing‖, International Journal of Application or Innovation in Engineering and Management (IJAIEM), Volume 1, Issue 2, October 2018.

[2] Cloud Security Alliances, —Top Threats to Cloud Computing V1.0‖, Cloud Security Alliances, Version 1, Page No. 3, March 2017.

[3] Wiiliam R Claycomb and Alex Nicoll,InsiderThreatstoNewResearchChallenges‖,CERT. Wayne A. Janssen, Cloud Hooks: Security and Privacy Issues in Cloud Computing , 44th Hawaii International Conference on System Sciences, January 2015.

[4] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and MateiZahria, A view of Cloud Computing‖, Communications of the ACM, Volume 53, Issue 4, April 2016.

[5] E. Kirda, C. Kruegel and G. Vigna, Cross- Site Scripting Prevention with Dynamic Data Tainting and Static Analysis‖, Proceeding of the Network and Distributed System. 2014.

[6] Shengmei Luo, Zhaoji Lin, Xiaohua Chen, Zhuolin Yang and JianyongChen,Virtualization Security for Cloud Computing Services‖,International Conference on Cloud and Service Computing, December 2011.

[7] Albert B Jeng, Chien Chen Tseng, Der-Feng Tseng and Jiunn-Chin Wang, A Study of CAPTCHA and its Application to user Authentication‖, Proceedingof2ndInternationalConferenceonComputational Collective Intelligence: Technologies and Applications, 2010.

[8] A. Liu, Y. Yuan and A Stavrou, ‖SQLProb:A Proxybased Architecture toward Preventing SQL Injection Attacks‖, SAC, March 2009.

[9] D. Gollmann, Securing Web Applications‖, Information Security Technical Report, Volume 13, Issue 1, 2008 153.

[10] ZouheirTrabelsi, Hamza Rahmani, Kamel Kaouech and Mounir Frikha, Malicious Sniffing System Detection Platform‖, Proceedings of the 2004 International Symposium on Applications and the Internet, 2004.

[11] Flavio Lombardi and Roberto di Pietro, Secure Virtualization for Cloud Computing‖, Journal of Network and Computer Applications, Academic Press Ltd. London, UK, Volume 34, Issue 4, July 2011.

[12] Hanqian Wu, Yi Ding, Winer C. and Li Yao,‖Network Security for Virtual Machine in Cloud Computing‖, 5th International Conference Information Technology, Seoul, December 2010.

[13] SAVVIS, Securing the Cloud A Review of Cloud ComputingSecurity Implications and Best Practices‖, VMWARE WHITE PAPER, SAVVIS.

[14] Ruiping Lua and Kin Choong Yow, Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network‖, IEEE Network, Volume 25, Number 4, August 2011.

[15] Ramaiah, Y. Govinda, and G. VijayaKumari. "Efficient public key homomorphic encryption over integer plaintexts." Information Securityand Intelligence Control (ISIC), 2012 International Conference on. IEEE, 2012.