WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A DATA STORAGE ARCHITECTURE CREATED WITH A FOCUS ON CLOUD SECURITY

Faizan Khan[1], Prof. Unmukh Datta[2]

[1] Computer Science Maharana Pratap Colllege of Technology Rajiv Gandhi Proudyogiki Vishwavidyalaya
[2] Computer Science Maharana Pratap College of Technology Rajiv Gandhi Proudyogiki Vishwavidyalaya

ABSTRACT

The success and popularity of cloud computing have increased due to current trends and technological advancements. Cloud computing offers on-demand services. Instead of using a single computer or a server on a local area network (LAN), cloud computing makes use of complex remote network sites and servers connected to the internet for data processing, management, and storage. Today, the study of data in the cloud and all security-related topics are prioritized, along with the preservation of statistics in cloud computing. It also covers the likely concern about data preservation in the cloud environment and the solutions used by various service providers to protect data security. Many applications benefit from data accessibility in the cloud. However, studies concentrate on the privacy of data perpetuation, which becomes more complicated with flexible data distribution among a dynamic user base. It calls for the efficient exchange of decryption keys amongst various authorized users and the concealing of information that has been outsourced. As a result, many approaches are available, some of which center on the combination of AES and attribute-based cryptography ABC.

Even though a technology has benefits, it also has drawbacks that are discussed on the site and can result in additional strain, such as CPU load, memory capacity, network load, or obstruction. The expansion of distributing the load across various nodes of a divided system to improve on different parts of the technology, which may be the best use of available resources and job rejoinder time, is known as load balancing. Therefore, load balancing is employed to prevent such issues by ensuring that each mainframe in the building or each node within the network performs approximately the same amount of work at any one time.

INTRODUCTION

The idea of adopting cloud computing as a utility is enticing all organizations to embrace this framework to adapt to a rapidly changing business landscape. In the IT industry, the most talked-about and transformative subject is cloud computing. IT managers aim to leverage cloud computing as a means to ensure scalability. IT infrastructures employ it to enable business flexibility. Cloud Computing began as a way for personal computing and has now become widely adopted for accessing online applications and storage, eliminating concerns about infrastructure expenses and processing capacity. Companies can transfer their IT infrastructure to the cloud and benefit from rapid scalability. However, it is crucial to understand the risks and threats present in a cloud environment, allowing for the development of an effective security policy for enhanced security measures. In order to deal with a rapidly changing business environment, every organization is being drawn to adopt cloud computing as a utility (M. Song, 2010). Cloud computing is the most talked-about and innovative topic in the IT industry. Cloud computing is a tool that IT managers wish to use in order to preserve scalability. According to L. IT infrastructures leverage it to enable business agility. Originally developed as a tool for interpersonal computing, cloud computing is now extensively used to access internet storage and applications without worrying about processing power or infrastructure costs (D. N. Chorafas, 2010). Companies can benefit from quick scalability by offloading their IT infrastructure to the cloud. However, in order to build an effective security strategy for improved security reasons, it is critical to comprehend the risks and hazards in a cloud environment (M. Song, 2010). Understanding cloud computing is the first step in preparation (L. Youse, 2008). Organizations must have a sufficient degree of trust in it in order to adopt it (Frank.A, 2011). To handle cloud security concerns including virtualization, tools, technologies, protocols, and human perceptions, a certain level of awareness was required. In this thesis, we examine the security of cloud computing and whether or not the public sector should employ cloud environments.

Objective :

The goals of the suggested work will be briefly described in this section.
New tools and protocols are suggested based on cloud security concerns after the current core technologies, procedures, tools, and protocols have been examined and analyzed.

The goals are :

1. To research current cloud computing techniques, fundamental technology, and tools.
2. To research and evaluate cloud service user security concerns.
3. To research and evaluate cloud service provider security concerns.
4. To suggest a new method for offering security in a cloud computing environment for both providers and users.
5. To develop and put into use user-side tools and provider-side and user-side protocols.

Security is the largest obstacle to the cloud paradigm. In this study, we created a tool and protocols that will help shift the way that cloud computing security is perceived and encourage future use of cloud computing by a variety of industries, including the military, government, and others, where privacy, data security, and dependability are critical and demand a high degree of security.

LITERATURE REVIEW

Service model : Depending on the services the cloud offers, cloud computing has been divided into three service models. A synopsis of each service model is provided below.

Applications are hosted by a vendor or service provider and made accessible to clients via a network, usually the Internet, under the software as a service (SaaS) distribution model. As new development techniques like Ajax and underlying technology supporting web services and service-oriented architecture (SOA) evolve, SaaS is becoming a more and more common delivery paradigm.Application service providers (ASPs) and on-demand computing software delivery strategies are closely related to software as a service (SaaS).

The hosted Similar to ASP, the application management (hosted AM) paradigm involves a provider hosting and distributing commercial software to clients via the Internet. Under the software on demand approach, the provider makes a single copy of an application designed especially for SaaS distribution available to clients via a network. The SaaS model has the following advantages.

Platform as a Service (PaaS) is an online method of renting network bandwidth, storage, operating systems, and hardware. Customers can rent virtualized servers and related services under the service delivery paradigm to run current applications or create and test new ones. Software as a Service (SaaS), a software distribution paradigm that makes hosted software programs accessible to clients via the Internet, gave rise to Platform as a Service (PaaS). PaaS offers developers a number of benefits. Operating system features can be regularly updated and modified with PaaS. Software development projects can be collaborated on by geographically dispersed development teams.

The cloud architecture gives the consumer the capacity to process, store, and use networks, as well as any software and operating system they like. Although the user has no control over the cloud infrastructure, they do have control over networking elements such as host firewalls, storage, operating systems, and installed apps. One type of service model is Infrastructure as a Service, which has Storage, hardware, and servers are among the equipment that a business outsources to support its operations.

Deployment Models : There are four deployment models concerning the services and users.

1) Private Cloud
2) Public Cloud
3) Hybrid Cloud
4) Community Cloud.

METHODOLOGY

Problem Statement : We read many research papers in which we found that there are still many cloud frameworks in which problems related to security and privacy still remain. So here we have developed a model that will provide advanced security and privacy protection in the cloud computing environment. Here we have tried to improve the performance of task scheduling based algorithms and also strengthen their data security.

Research Methodology : The science of carrying out research or methodically resolving research issues is known as research methodology. We can employ a variety of pertinent approaches or strategies to accomplish the intended research goal [C.R. Kothari, 2004].
These approaches are:

1. Review of Literature
2. Survey
3. Survey Outcome
4. Issue resolution (Research work)

Literature Review : In order to find pertinent content, we have gathered data for Literature from a variety of sources, including IEEE, Blekinge, Institute of Technology, Springer, CSI, Inderscience, and ACM. However, we used a wide range of additional materials, including books, journals,

white papers, and online resources from Google, Microsoft, Amazon, EMC, NetApp, OpenStack, and Eucalyptus, as well as the IBM cloud. Information regarding the cloud and other cloud-related technologies has been gathered by us.

Survey : We featured interviews with various IT professionals from the government, cloud news, IT business news, IT companies, military, universities, schools, colleges, and IDC. We created the questionnaire with our primary goals in mind.

Data Collection Sources : We study books, periodicals, journals, ancient software, tools, company databases, and direct and indirect questions from IT personnel.

Designing Questionnaire : To accomplish our goals, we created a questionnaire based on the results of the literature research. We created the questionnaire so that it would precisely answer our study questions. We had numerous discussions with our managers and coworkers prior to completing our questionnaire.

Selected Audience : We focused on IT professionals, network administrators, system assistants, network consultants, software developers, students, penetration testers, network security analysts, network and system officers, and others for our study after reviewing the literature and consulting with our colleagues.

Result of Survey : According to the survey, individuals are not prepared to embrace cloud since it is not secure, and security is the biggest obstacle in the cloud. According to the poll, 87.5% of respondents claimed that because cloud computing is not secure, they cannot use it as an organizational tool.

Overview of the Research Project : We conducted research and created tools and standards for cloud security in order to address the survey results. They are created and implemented for several user and server-side levels in this work. The next chapters provide specifics on these tools and protocols.

1) User Security Tool for Cloud Services.
2) Cloud Security Protocol and Multilevel Security Framework.
3) Protocol for Data Storage.

User Security Tool for Cloud Services : Starting with secure level communication to the user, this tool offers a number of security features and capabilities. Oracle database 12c is used for data encryption. Any cryptosystem can be applied here. However, our approach uses the AES cryptosystem. ECLIPSE, Java, and JSP are used in the implementation of this program.

EXPERIMENT, RESULT & DISCUSSION

DATA STORAGE GUIDELINES FOR ENSURING CLOUD SECURITY

Data privacy and verification within cloud environments have been thoroughly explored in numerous existing studies. Upon reviewing the area of public auditability, it becomes clear that the vulnerability of third-party auditors has not been adequately addressed. Prior research tends to overlook all security risks and primarily focuses on scenarios involving a single server. Additionally, many do not account for dynamic data operations, and the challenge of ensuring both public auditability and dynamism has been only recently tackled, highlighting the risks associated with having third-party auditors. The DSP Protocol has been introduced to enhance the security of data in cloud environments by enabling remote verification of data and its integrity on the server.

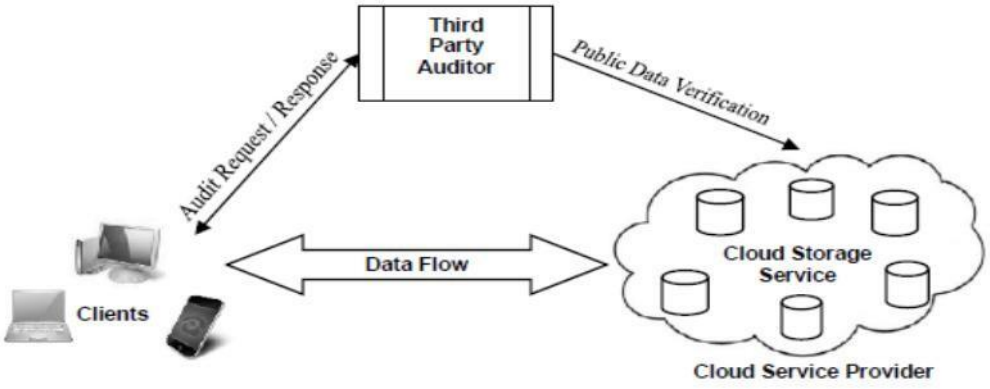


Figure24: Configuration of third-party data auditing in the cloud

Proposed Work

The Data Storage Protocol (DSP) has been created to enhance the security of data stored in cloud environments by verifying the data and its possession on the server remotely. The DSP protocol enables users to receive a probabilistic proof from the storage service providers, which serves as evidence that their data has been securely stored. One benefit of this protocol is that the storage service provider can generate the proof by accessing only a small portion of the entire dataset. The data owner implements the protocol to confirm that a dataset is held on a server machine as a collection of n blocks. Before the data is uploaded to the remote storage, the data owner processes the dataset beforehand and generates a piece of metadata. This metadata is kept on the data owner's side while the dataset is sent to the storage server. The cloud storage service retains the dataset and responds to future queries from the data owner by providing the necessary data.

The data owner (client) may perform operations on the data, such as expanding it or creating additional metadata to be stored on the cloud server. Before deleting the local copy, the data owner can execute the Data Storage Protocol (DSP) to ensure that the uploaded version has been successfully stored on the server machines. The DSP utilizes two methods:

1. Metadata Generation
2. Metadata Verification

This approach addresses the issue of preventing third-party auditors from accessing the data directly. The Data Storage Protocol (DSP) is intended for the specific purpose of granting access only to the owner-related metadata of the data being verified.

Purpose of DSP Protocol :

(a) Off-Site Data Ownership at Unreliable Storage Facilities

This study indicates that cloud storage can successfully achieve the objective of obtaining all storage resources in a plug-and-play manner, which has become a focal point of interest. When individuals store their data in cloud storage, their primary concern is often whether the data remains intact. The purpose of the DSP protocol is to verify data possession remotely. Here, we introduce an effective Remote Data Possession Check (RDPC) scheme that offers several benefits.

(b) Public Verifiability for the Security of Storage :

This paper indicates that data outsourcing can alleviate the burden of local data storage for users. It also removes their direct control over the reliability and security of storage, which has historically been a concern for both businesses and individuals.

This novel approach introduces various new security challenges that must be clearly understood and addressed. This paper examines the issue of maintaining data integrity in Cloud Computing. To validate the accuracy of the data, we explore the role of a third-party auditor who can verify the integrity of the data stored in the cloud on behalf of the cloud consumer. The DSP protocol ensures minimal storage requirements on the client side, which will be advantageous for clients.

(c) Public Verification for Storage Protection :

The challenge lies in ensuring the integrity of data storage in cloud computing. It addresses the need for a third-party auditor to verify the integrity of dynamic data stored in the cloud. This not only enables public auditability but also supports dynamic data operations. It begins by highlighting the challenges and potential security risks associated with directly extending fully dynamic data updates based on previous research, and then demonstrates how to develop a refined verification scheme for the smooth integration of these two critical features in our protocol design.

(d) Remote Data Verification through Provable Data Ownership

Presents a framework for verifiable data presence that can be utilized for remote data verification. The framework creates probabilistic proofs of possession by selecting random sets of data blocks from the server, significantly decreasing I/O expenses. The challenge/response method transmits a minimal, fixed amount of data, thereby reducing network communication. Additionally, the framework is resilient and includes strategies for addressing varying levels of data corruption. It introduces two provably secure PDP schemes that outperform earlier approaches in terms of efficiency. Notably, the server's overhead is minimal (or even constant), unlike previous solutions that had linear overhead based on data size. It also suggests a generic transformation that enhances the robustness of any remote data verification approach founded on spot checking, and carries out a comprehensive experimental analysis to explore the balance between performance, security, and space overhead when enhancing robustness in the remote data verification scheme.

(e) Data Integrity Verification with Privacy Protection

A third-party auditor allows for periodic checks of the data stored by a service and helps in ensuring the data is returned in its original form to the customer. The protocols maintain privacy, meaning that the contents of the data are never disclosed to the auditor. This approach shifts the responsibility of verification away from the customer, easing the concerns of both the customer and the storage service regarding data leaks, and offers a means for independent arbitration of data retention agreements.

Data Storage Protocol

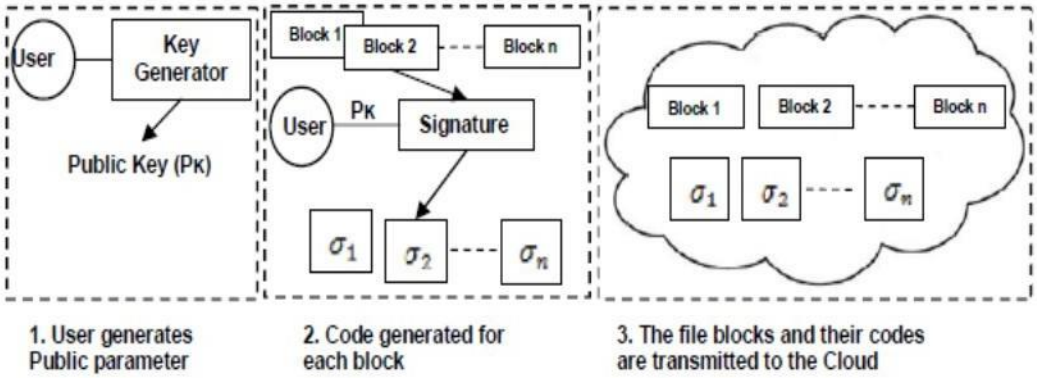
The security model is fundamentally structured as a data integrity framework that facilitates the incorporation of public auditability alongside dynamic modifications. This scheme authenticates metadata instead of the actual data. The model consists of two primary components.

(a) Metadata Generation and

(b) Metadata Verification

(a) Metadata Generation

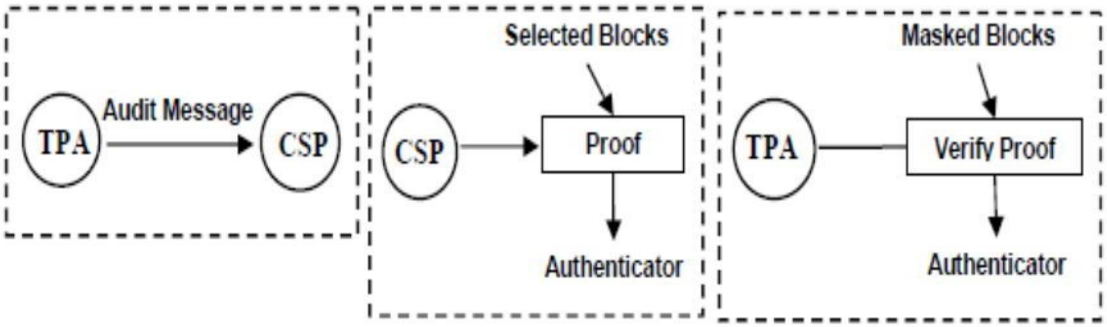
The process begins with the cloud client creating a public key parameter, denoted as Pk. Next, the client generates a signature for each individual file block. This signature serves as a type of metadata that combines the public key with the file blocks, referred to as codes. Ultimately, the created metadata is sent to the cloud storage.



Metadata Generation

(b) Metadata Verification

Once the metadata is transmitted to the cloud, the Third Party Auditing (TPA) is able to conduct data verification at any time. When the TPA gets a request from the client for data verification, it issues an audit message to the service provider asking for a specific set of data blocks. This audit message includes the positions of the blocks being requested. The service provider creates a linear combination of the blocks and applies a mask. The service provider then sends the authenticator along with the masked blocks to the TPA. Ultimately, the Third Party Audition (TPA) evaluates the masked blocks provided by the service provider alongside the metadata supplied by the client.



Metadata Verification

DSP Protocol Algorithm :

Start
Metadata generation( )
Step 1: Start breaking down the file F into blocks.
Step 2: Create a public key Pk.
Step 3: Produce authentication codes for each block using the key.
Step 4: Send the authentication codes together with the file blocks to the cloud.
End

Start
Metadata verification( )
Step 5: Create an audit message that includes the positions of the file blocks and send it to the CSP.
Step 6: Relay the response message containing the metadata of the requested blocks to the TPA.
Step 7: Check the metadata received from the CSP against the data from the client.
End

Data Storage Protocol Equations

Pk represents the public key used for the encryption of file blocks.
σ denotes the code generated for each block, also known as metadata.

Fb refers to the actual file that requires verification.
B stands for a single block of the file.
Equation 1 illustrates how the file is segmented into blocks.

$$F \rightarrow \sum B1 + B2 + \cdots + Bn$$

Equation 2. Code generated for each block.

$$B_1, B_2, \ldots, B_n \xrightarrow{P_s} \sigma_1, \sigma_2, \ldots, \sigma_n$$

Equation 3. Code and blocks are moved to the cloud.

$$B_1, B_2, \ldots, B_n + \sigma_1, \sigma_2, \ldots, \sigma_n \longrightarrow \text{CSP}$$

Equation 4. TPA dispatches an audit notification to CSP.

$$\text{TPA} \xrightarrow{\textit{Audit Message (File F, Pos)}} \text{CSP}$$

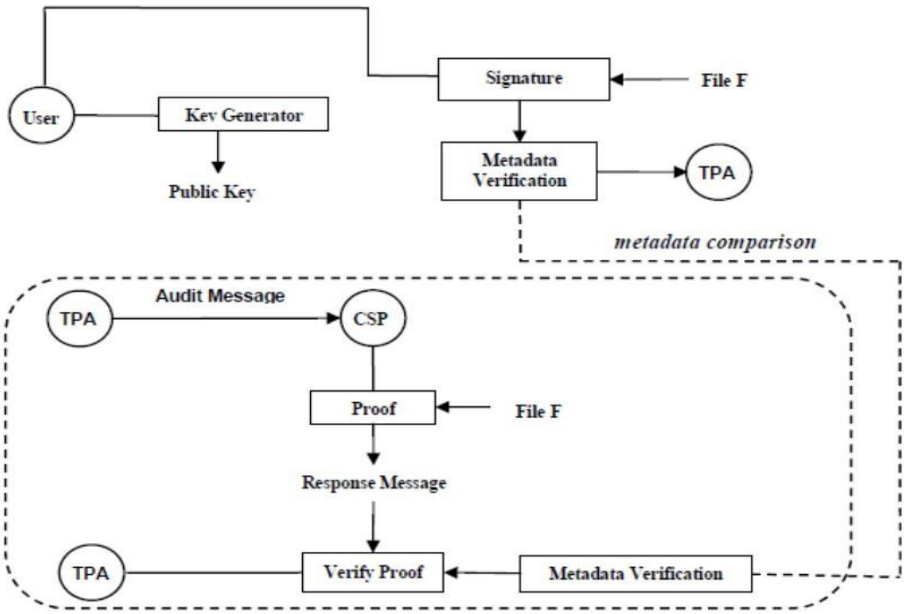
Equation 5. CSP transmits obscured blocks, while TPA sends a verification message to CSP.

$$\text{CSP} \xrightarrow{\textit{Masked Blocks + Authenticator}} \text{TPA}$$

Equation 6. CSP transmits masked blocks, while TPA sends an audit message to CSP.

Operation

Metadata Verification Operations



Implementation

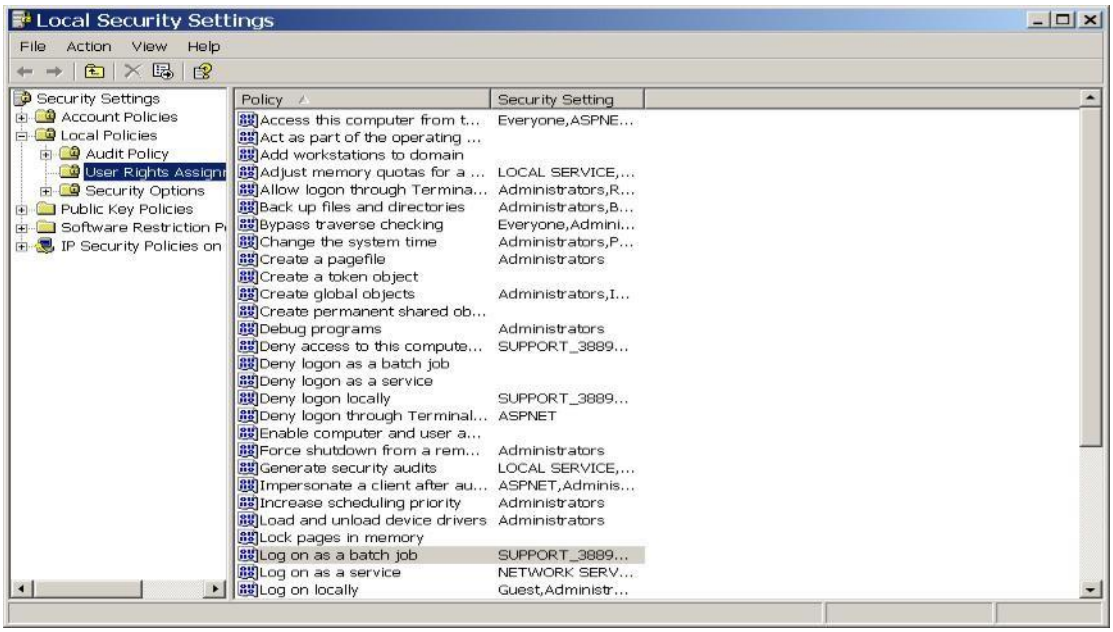
(a) Operating Systems Meta data

The operating system keeps track of metadata to verify user identities; to do this, an account is established or a batch file is invoked by creating an object. This account allows the user to link to the Metadata Server. The Metadata Server can approve or reject the user's request for access to metadata objects depending on the authentication status.

Below are the steps to create a metadata object.

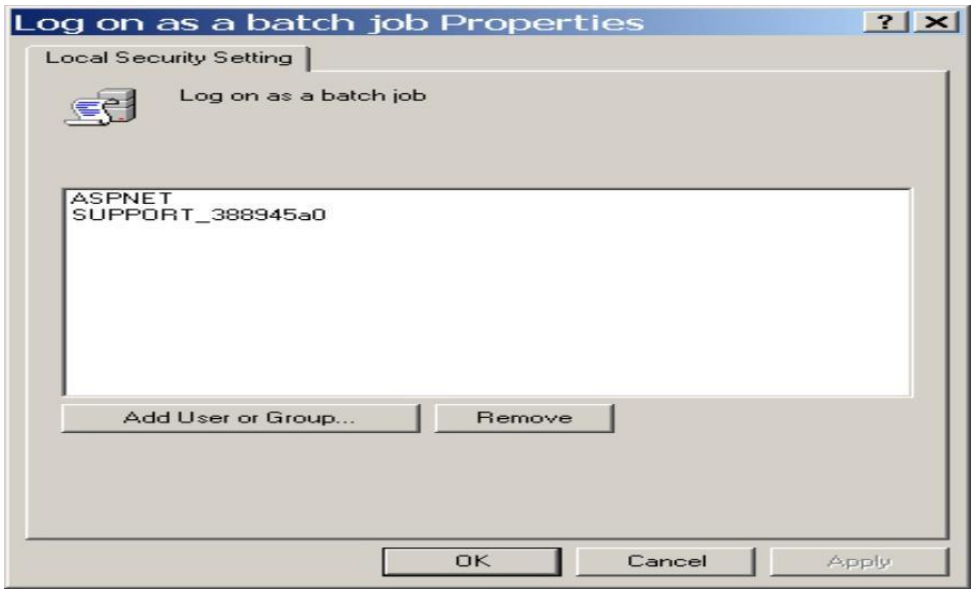
1. Click on Start, then go to Settings, followed by Control Panel, then Administrative Tools, and finally select Local Security Policy.
2. In the Local Security Settings window, expand the Local Policies section in the left pane and select User Rights Assignment.

(Example for Metadata Development)



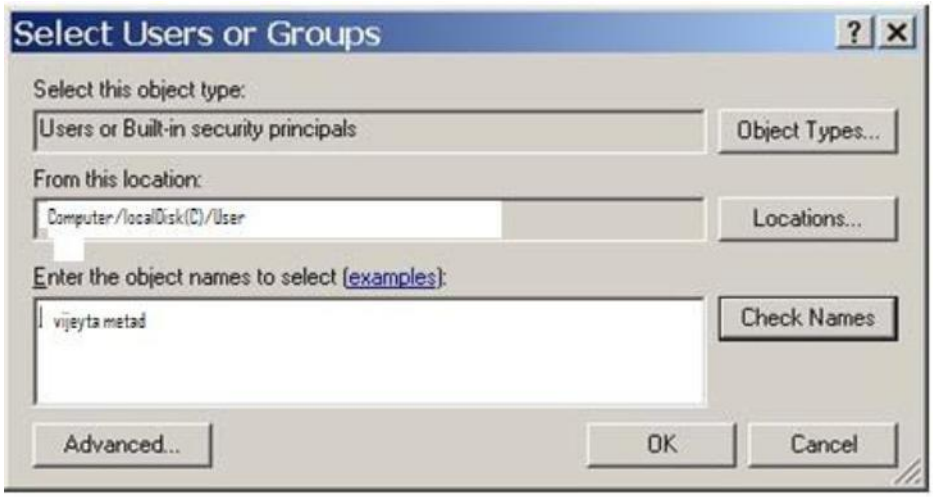
User Rights Allocation

2. Select the Logon as a batch job option in the right pane to open the Properties dialog box for Logon as a batch job.



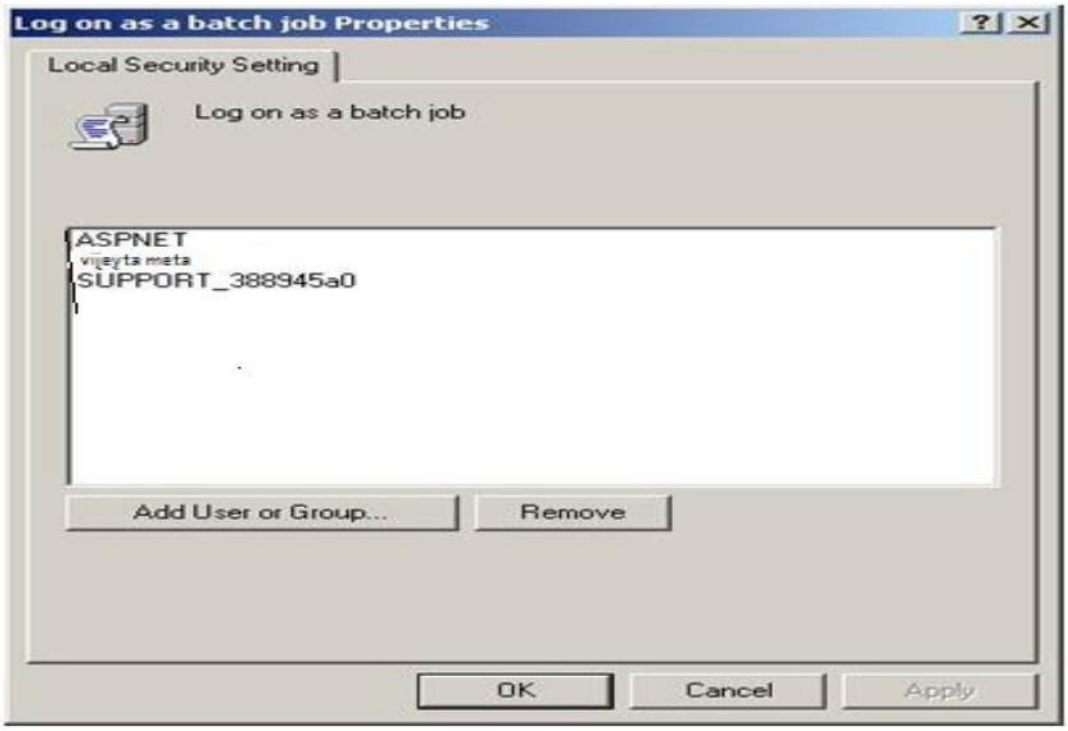
Batch job Properties

3. In the Local Security Setting tab, click on Add User or Group to open the Select Users or Groups dialog box. Input your information in the provided fields and select OK to go back to the Properties dialog box for logging on as a batch job.



Generate User or Group Metadata

4. Ensure that your new group is visible in the box on the Local Security Settings tab, then click OK.



A New Group Emerges

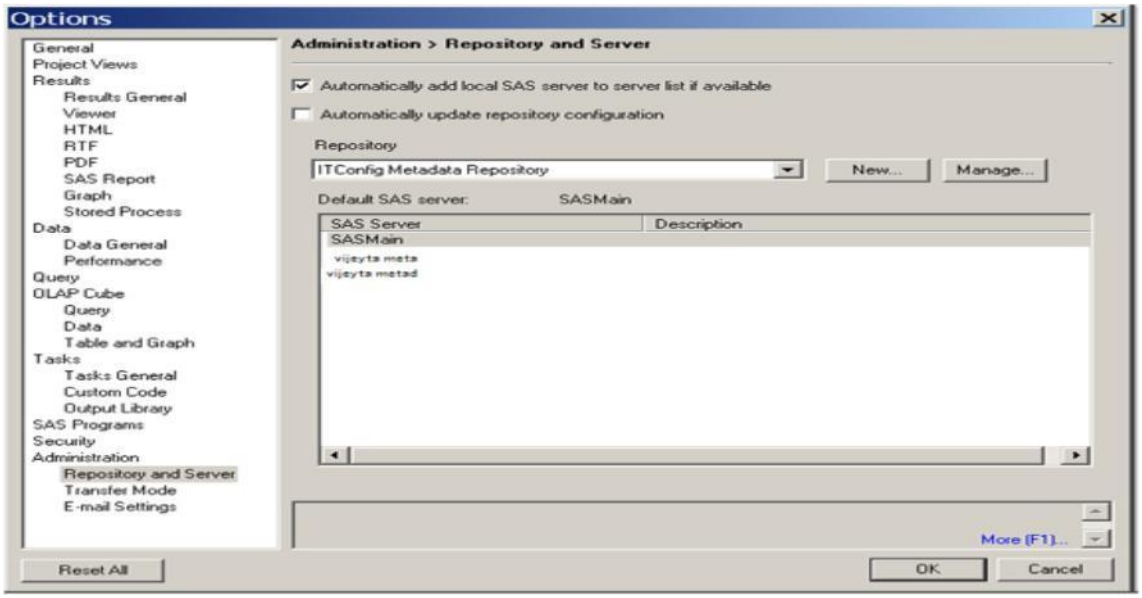
(b) Verify Metadata

1. Launch Enterprise Guide.

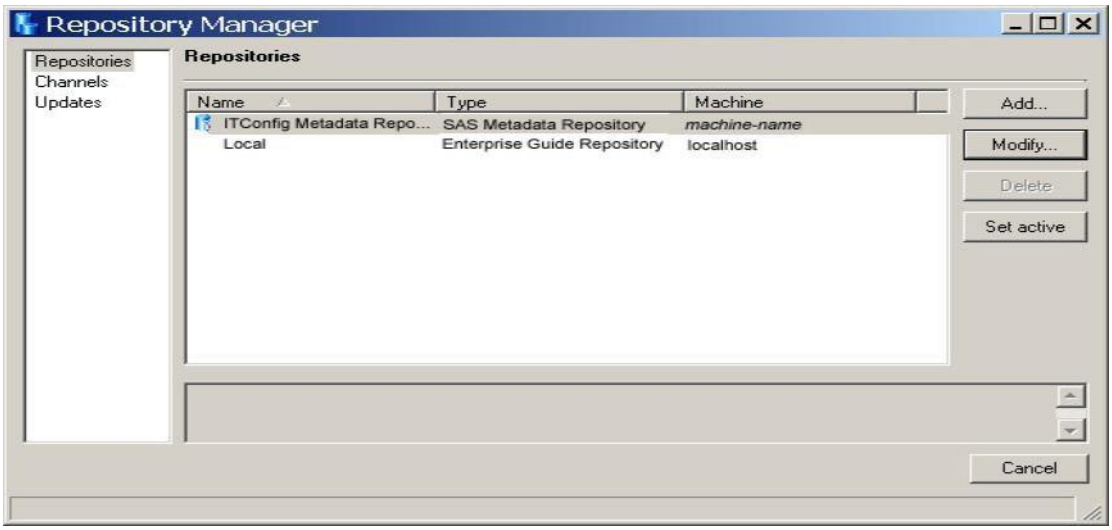
2. Navigate to Tools ► Options ► Administration ► Repository and Server. In the dialog box for Repository and Server, click Manage to open the Repository Manager.

3. In the Repository Manager, choose the ITConfigMetadataRepository entry and then click Modify to open the Modify Repository dialog box.

Sample for Verification



Verify Metadata



Metadata Repository

4. In the Modify Repository dialog box, ensure that the repository is set up as follows:
   - Machine: The Remote option is selected, and the machine name of the Metadata Server has been entered.
   - Port: 8561
   - UserID: Use DEMO for testing purposes or the appropriate user ID for a production client.
   - Password: Enter the password associated with the user ID (either DEMO or a valid production client user ID) that you utilize.

   Then click Browse to connect to the Select Repository dialog box...

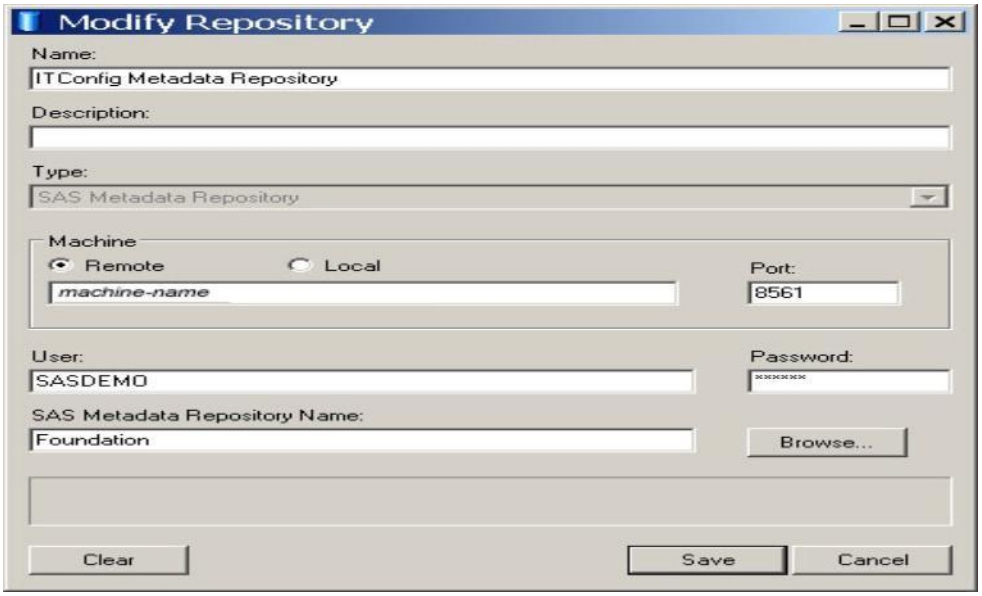


Figure34: Metadata Server Details

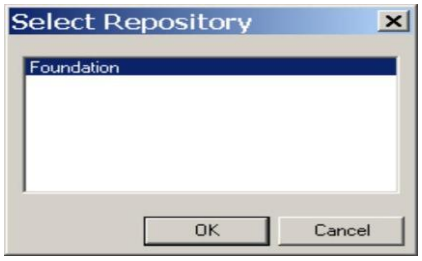


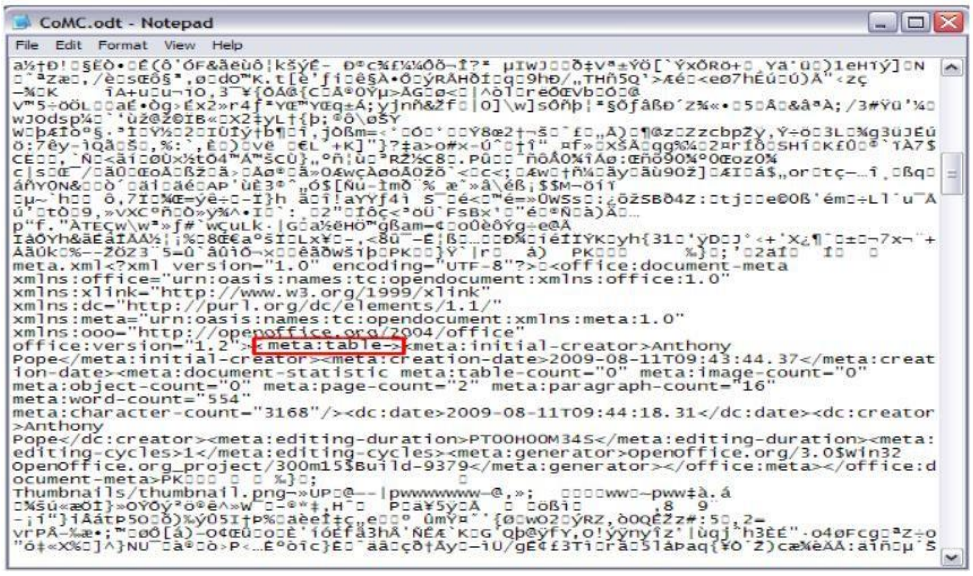
Figure35: Metadata Found

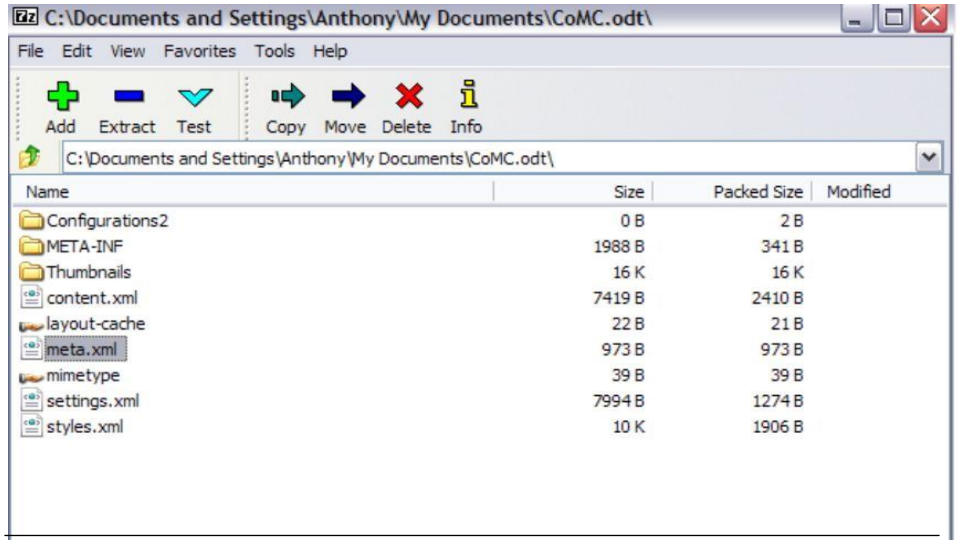
(c) Create a copy of Metadata by XML at user Machine

1. In the Catalog window, right-click on the folder where you wish to save the metadata template.
2. Select New > XML Document. A new XML file with the default name metadata.xml will be created in that folder.
3. Enter a suitable name for the metadata template (metadata.xml).
4. Press ENTER.
5. The file, Metadata.xml, currently contains no information to show in the description tab.
6. Click the Edit button located in the description tab.
7. Provide suitable content for this metadata template.
8. 8.Click the Save button in the description tab to display the contents of the metadata template.

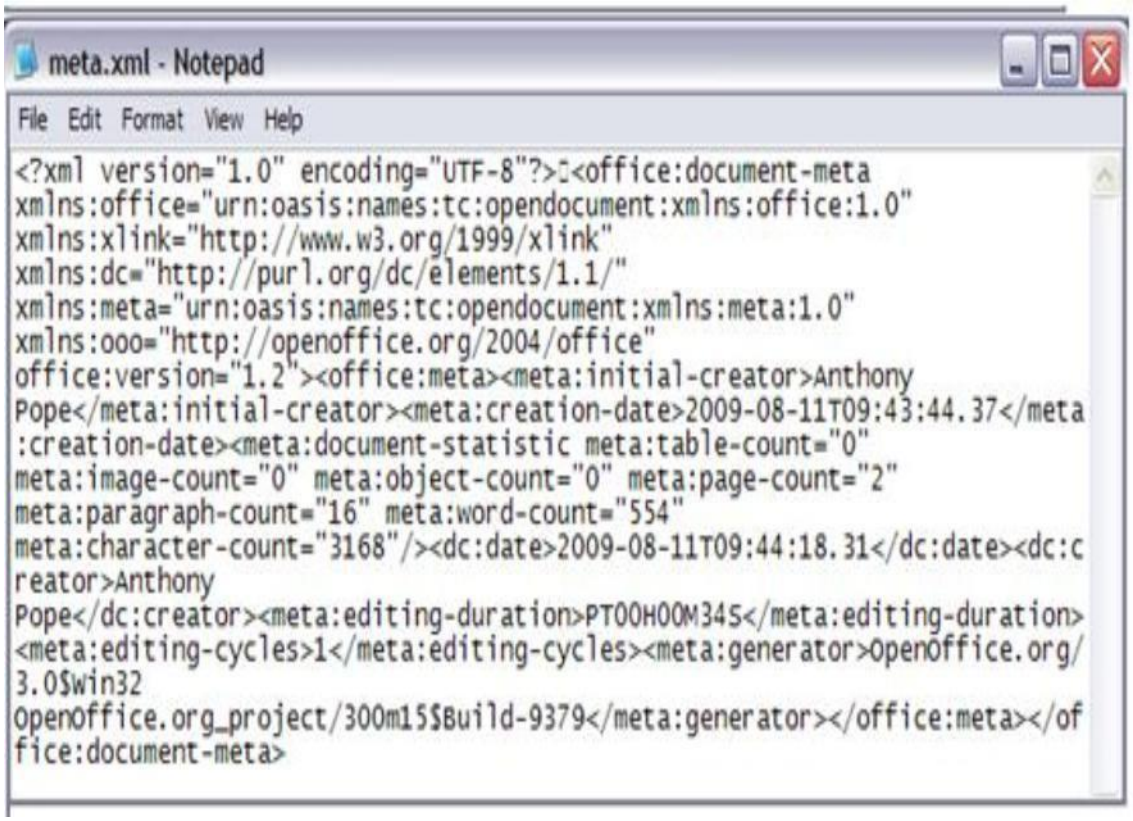
Meta data Sample with xml file

Meta data from batch Job of O/S





Metadata document creation



A comprehensive explanation of Metadata.

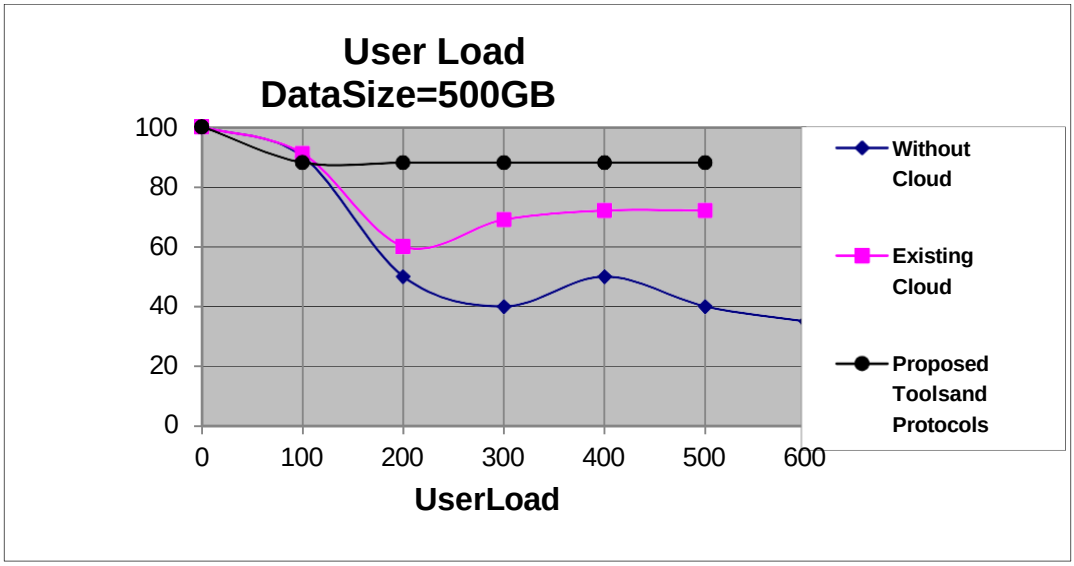
CONCLUSION :

The DSP protocol enables users to acquire a probabilistic proof from storage service providers. Metadata verification is formulated for this purpose and limits third-party access to the metadata associated with the data to be verified. The Data Storage Protocol can be improved further to assess security, the auditor's trustworthiness, and the confidentiality in managing the data without any bias. Additionally, the data stored in the cloud can be encrypted, and the unique code generated for individual files can be transmitted using secure transmission protocols.

Results :

The results were compared with existing tools, proposed tools, and protocols from organizations of various sizes and workloads. Our findings specifically targeted an organization to bridge the gap in their understanding of cloud and security issues in traditional IP networks and the cloud

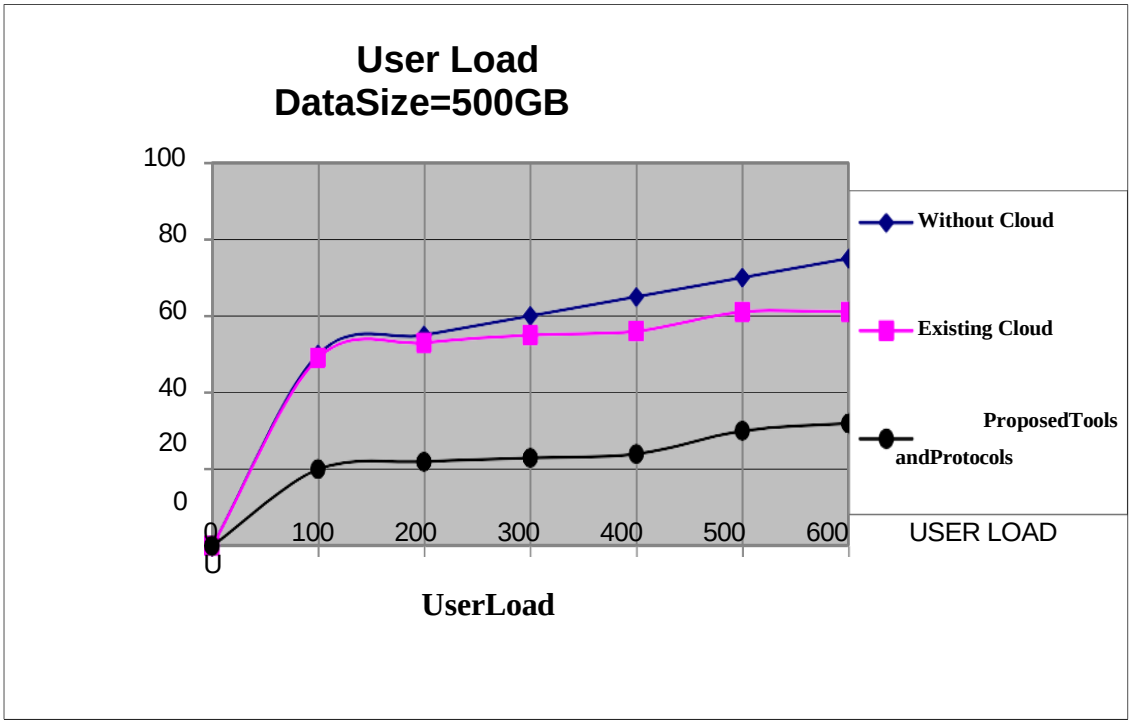
environment as a whole. The primary emphasis of these results was to gain insight into an organization and the respondents' perspectives on scalability, complexity, security concerns, current expenses, expected savings, types of data, and access control mechanisms. We will explore all of these topics in the following section. This work will provide clarity on how organizational needs align with the benefits of cloud services and how professionals view some of the challenges and their solutions. Below are the results of our study.



Scalability Comparison Chart

Complexity :

The current system's complexity is assessed at 61%, indicating that it is somewhat challenging to sustain. The findings indicate that the complexity of organizations is diminished with the suggested tools and protocols.



Graphs for Comparing Complexity

Discussion

This thesis has thoroughly discussed the execution of a cloud environment for a secure organization where data is susceptible to security threats. We have structured our work so that we can initially determine the reasons for utilizing cloud infrastructure and subsequently provided specifics about one of the techniques and tools employed for its implementation. We aimed to supply sufficient evidence to encourage them to utilize cloud-based services within their network.

CONCLUSION AND FUTURE SCOPE

CONCLUSION :

This research emphasizes the findings from our study to draw a conclusion aimed at addressing our research questions. Based on the findings of this study, cloud computing can be embraced by any industry where data is susceptible to security risks, such as IT firms, government entities, or military organizations, allowing them to safeguard and oversee their information flow. Findings are presented to determine which technology meets our objectives and to grasp the overall viewpoint of IT professionals regarding the transition to cloud technology.

This effort delivers the outcome needed to foster trust among various organizations in cloud technology. The literature review consists of an in-depth examination of cloud computing overall and specific security concerns along with identified vulnerabilities. It also emphasizes security awareness and delves into virtualization specifics, along with practical security concerns such as cross VM attacks and VM migration threats. All this effort has enabled us to create an improved environment for IT companies/governments. From our efforts, we obtained specific results that aided us in reaching a conclusion.

Future Work :

This study offers the data required for implementing cloud infrastructure in emerging organizations. We offered the current market trends along with technologies that are affordable, dependable, efficient, and safe. Future research efforts should concentrate on migrating a small segment of the network with public data to a cloud for experimental purposes, enabling further exploration. In the future, this study could be expanded to standardize cloud computing, which is now integral to all organizations. This would allow for feedback at the domain and CSP levels, enabling us to identify the attack path at a specific point in time along with attack alerts.

REFERENCES

1. Rashmi and Dr.G.Sahoo. *International Journal on Cloud Computing: Services and Architecture (IJCCSA)* ,**Vol.3, No.4, (2013).**
2. Abdulaziz , Architecture of cloud computing ,*International Journal of Business and Social Science* **Vol. 3 No. 1, (2012).**
3. Zhifeng Xiao and Yang Xiao, Security and Privacy in Cloud Computing *in IEEE communications surveys & tutorials***, 1553-877X/12/, pp1-17, (2012).**
4. B. Grobauer, T. Walloschek, and E. Stocker, Understanding cloud computing vulnerabilities, *Security and Privacy, IEEE,* **vol. 9, no. 2, pp. 50-57, (2011).**
5. C.Wang,K.Ren,J.Wang,SecureandPracticalOutsourcingofLinearProgrammingin Cloud Computing, *In IEEE Trans. Cloud Computing* **April 10-15, (2011)**.
6. Frank,A.Oludele,andothers,CloudComputingSecurityIssuesandChallenges, *InternationalJournalofComputerNetworks(IJCN)*,**vol.3,no.5,p.247, (2011)**.
7. Jansen, W., & Grance, Guidelines on Security and Privacy in Publics CloudComputing. *Information Technology Laboratory, Gaithersburg,* United States of America: *National Institute of Standards and Technology***, (2011).**
8. S. Ortiz, The Problem with Cloud-Computing Standardization, in *IEEE Journal on Computer*, **vol. 44, pp. 13-16**, **(2011)**.
9. Sahoo,S.Mohapatra,and R.Lath,Virtualization:A Survey onConcepts,*Taxonomy and Associated Security Issues*, **pp. 222–226,(2011)**.
10. NewsBriefs,Amazon'sMassiveCloudHostingSiteCrashes,*JournalofIEEE Computer*, **Vol. 44, pp. 18-20,(2011**).
11. W Jansen, T Grance ,NIST Special Publication,csrc.nist.gov *Page 1.Guidelines on Security and Privacy in Public Cloud Computing,* **Publication 800-144 ,(2011).**
12. H.Takabi, J.B.D.JoshiandG.Ahn,Securityandprivacychallengesincloud computing environments, *Security & Privacy, IEEE,* **Vol. 8, no. 6, pp. 24–31,(2010).**

13. KaiHwang;DeyiLi,TrustedCloudComputingwithSecureResourcesandData Coloring, *Internet Computing, IEEE* , **Vol.14, no.5, pp.14-22,(2010).**

14. R.Chakraborty,S.Ramireddy,T.S.Raghu,H.R.Rao,TheInformationAssurance Practices of Cloud Computing Vendors, *IT Professional*, **Vol.12, pp.29-37,(2010).**

15. Luis M. Vaquero, Luis Rodero-Merino and Daniel Mor´an, Locking the sky: a survey on IaaS cloud security, *Computing*, **(2010).**

16. R.Chakraborty,S.Ramireddy,T.S.Raghu,H.R.Rao,The*InformationAssurance Practices of Cloud Computing Vendors*, *IT Professional*, **Vol.12, pp.29-37,(2010).**

17. Qian Liu, Chuliang Weng, Minglu Li, Yuan Luo,An In-VM Measuring Framework for Increasing Virtual Machine Security in Clouds, *Security & Privacy, IEEE*,**Vol.8, no.6,pp.56-62,(2010).**

18. H. Takabi, J. B. D. Joshi, and G. Ahn, Security and privacy challenges in cloud computing environments,*Security & Privacy, IEEE*, **vol. 8, no. 6, pp. 24–31,(2010)**.

19. Y. Chen, V. Paxson, and R.H. Katz, What's New About Cloud Computing Security?" tech. report UCB/EECS-2010-5, *EECS Dept., Univ. of California, Berkeley*, **(2010).**

20. R. A. Lumley, *Cyber Security and Privacy in Cloud Computing, Multidisciplinary Research Problems in Business***,(2010).**

21. Kai Hwang and Deyi Li, Trusted Cloud Computing with Secure Resources and Data Coloring, *Internet Computing, IEEE* , **vol.14, no.5, pp.14-22,(2010).**

22. Sahoo, S. Mohapatra and R.Lath,Virtualization: *A Survey on Concepts, Taxonomy and Associated Security Issues*, **pp. 222–226, (2010).**

23. H. Takabi, J.B.D. Joshi, G. Ahn, Security and Privacy Challenges in Cloud Computing Environments, *Security & Privacy, IEEE* , **vol.8, no.6, pp.24-31, (2011).**

24. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, *Journal of Future Generation Computer Systems*, **25:599-616, (2009).**

Websites :

1. https://www.cloudzero.com/blog/cloud-computing-statistics/

Books :

1. https://industri.fatek.unpatti.ac.id/wp-content/uploads/2019/03/210-Cloud-Computing-Sandeep-Bhowmik-Edisi-1-2017.pdf
2. https://api.pageplace.de/preview/DT0400.9781482205442_A24097357/preview-9781482205442_A24097357.pdf