JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 07, ISSUE 01, 2020

ANALYSIS ON PERFORMANCE SCALABILITY AVAILABILITY AND SECURITY IN VARIOUS CLOUD ENVIRONMENT SYSTEMS

ATHMAKURI NAVEEN KUMAR

Senior software engineer, software developers industry, GLOSOFT Technologies PVT LTD, Hyderabad, India

Email id: shanvinaveen5@gmail.com

ABSTRACT:

Cloud computing refers to the sharing of resources and computing tasks among a network of computers. Cloud computing enables us to do all of these things by utilising remote servers to transmit, store, and retrieve information. Because of the vast number of Virtual Machines available in the cloud, we now have the chance to perform parallel computations. The biggest threats to cloud computing may now come from its performance, scalability, availability, and security. In this article, we'll discuss the challenges of scalability, availability, and security in the context of cloud computing, and outline the steps we've taken to improve the safety and reliability of our infrastructure in this setting. Also, we stress cloud computing's elasticity. Also covered will be some of the key factors in achieving the promised high performance of cloud computing.

1. INTRODUCTION

1.1 Background

The popularity and success of cloud computing has been predicted by the direction of recent trends and technological advancements. This new approach has been popular in metropolitan areas because it provides a cost-effective framework that aids in data storage, processing power, and programme development. Inefficient data control technique on the part of these gifted storage devices has led to a plethora of challenging design difficulties. The security and efficiency of the cloud system are significantly influenced by two obstacles: data privacy and data reliability. Cloud computing's appealing economics mean that users need only pay for the resources they really employ, rather than for unused capacity they never need to worry about. Everything is made available at any time, in any location, for everyone to utilise. There won't be any problems like that when using it.

The cloud computing paradigm has grown in popularity as a useful tool because it facilitates ubiquitous, on-demand access to a shared pool of configurable computing resources, including hardware, operating systems, networks, servers, storage, applications, and services. Cloud computing is sometimes defined as "a solution of network for supplied that affordable, trustworthy, uncomplicated, and straight forward permission to IT resources," which is a popular and straightforward explanation. Cloud computing is formally defined as follows by the US National Institute of Standards and Technology (NIST):

The term "computation in the cloud" refers to a service that makes a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) readily available and visible to users with minimal intervention from the users themselves.

ISSN- 2394-5125 VOL 07, ISSUE 01, 2020

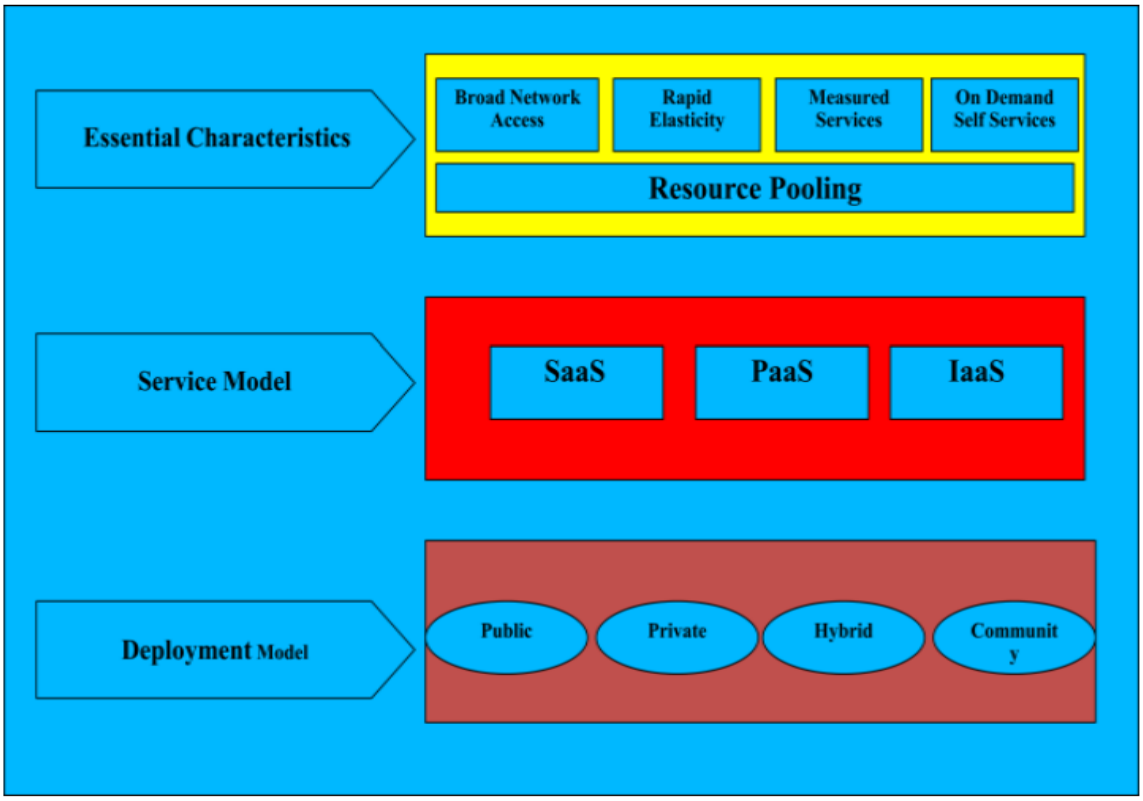


Fig. 1. A conceptual view of computing in cloud

The term "cloud computing" refers to a type of distributed computing that is dynamically configured and made available on demand. The new paradigm of massively scalable networks is distinct from the norm of conventional systems. Providing three tiers of service requires a great deal of abstraction.

Some cloud-based systems are dependent on the deployment model chosen, which can be either private, public, or a mix of the two. It's a hybrid system that uses both computer hardware and software, and it comes equipped with the three essential components needed to provide cloud services.

2. LITERATURER EVIEW

AES, DES, 3DES, Blowfish, RC4, IDEA, and TEA are just few of the common symmetric algorithms compared in terms of performance by Wani et al. [1].

As Basu et al. Discussions of access control systems, their proper connectivity, and the remaining set of unresolved problems in this sector round out [2]'s coverage of cloud security, virtualization difficulties, and solutions.

As Kaura et al. [3] Discussion of cloud services, potential dangers, and safety precautions

Authors Shanmugasunda ram et al. [4] Discussion of cloud, infrastructure, access control, third-party privacy, confidentiality, reliability, and data integrity security requirements. It depicts methods used to handle cloud security vulnerabilities and the difficulties associated with doing so.

ISSN- 2394-5125 VOL 07, ISSUE 01, 2020

Based on work by S. Kaushik et al. [5] Cloud-related assaults, threats, hazards, and security problems are outlined along with the preventative steps that can be taken to address them. The impact of various network assaults on various cloud frameworks has also been explored in the present study.

Security concerns, limits of current methods, and potential remedies are discussed by Mehra N. et al. [6].

M. Manoj Kumar et al. [7] Using different metrics of design debt, we can isolate the sources of cloud computing's design debt. While it's possible that a cloud-based service with unfinished, untested code that's available online may function well and be acceptable to users, this is not guaranteed.

Authors Timothy D.P. et al. [8] Developing a novel security approach for protecting cloud-stored data by utilising a hybrid cryptosystem. robust protection for data sent over the internet and instantaneous, trouble-free access to a pool of useful computing resources, namely the web, servers, and storage software, on demand.

R. Barona and colleagues [9] Cloud computing, various cloud models, and the key security concerns and data breach issues currently being investigated inside the cloud computing framework are introduced. data breach in the cloud: an investigation of the relevant research and challenges presents, with recommendations for service providers and an initiative to influence cloud servers to improve their key worry in the current economic climate.

The work of S.K. Sahil Sood et al. [10] Through a pay-as-you-go online service model, "cloud computing" provides scalable virtual computer resources.

3. SAFETY ISSUES AND APPROACHING IN CLOUD COMPUTING WITH LOAD BALANCING ALGORITHM

Information security requirements for the cloud should include a number of the topics outlined by ISO (International Organization for Standardization). In addition, this is where cloud computing security may provide direction in becoming a truly remarkable and safe technological solution. Parameters that must be met for public cloud, private cloud, and hybrid cloud data security are depicted in figure 2. Optional and required security measures are broken down in this diagram, along with cloud service descriptions for each

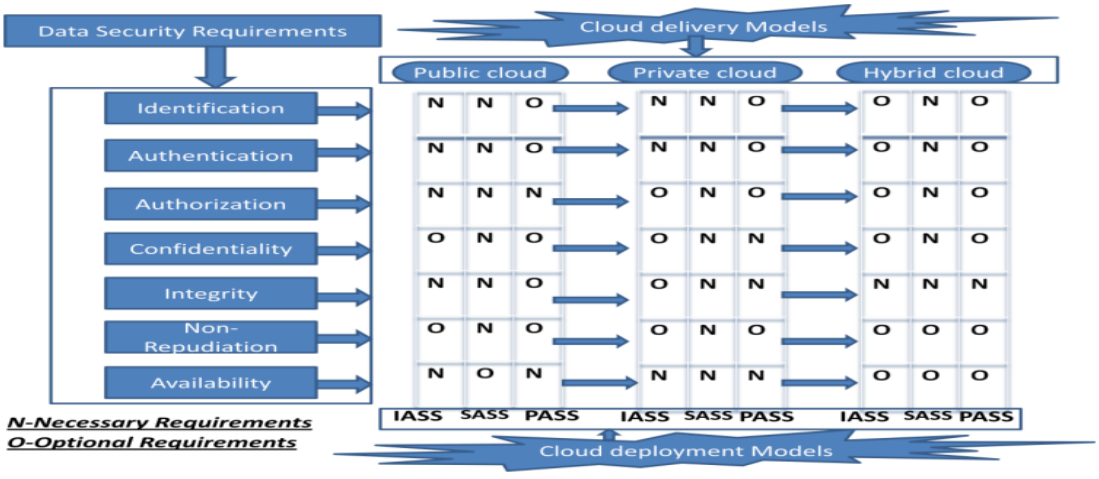


Fig. 2 Security requirements in computing of cloud.

ISSN- 2394-5125 VOL 07, ISSUE 01, 2020

To illustrate the intertwined nature of information security, cloud deployment and delivery approaches are shown in Figure 2. Figure 2 compares the multiple cloud delivery and deployment methods to the information security requirements, with "N" representing the required requirements and "o" representing the recommended requirements.

3.1 Security Algorithms and its parameters

The encryption method is just one of many that must be considered for data security in cloud computing. The potential for data loss is conditional on the following factors.

A. Reset of data

B. Transit of data

A. Reset of data

Resetting of data occurs when a user of cloud storage retrieves their data via the internet. This method utilises real-time data, as opposed to previously saved copies.

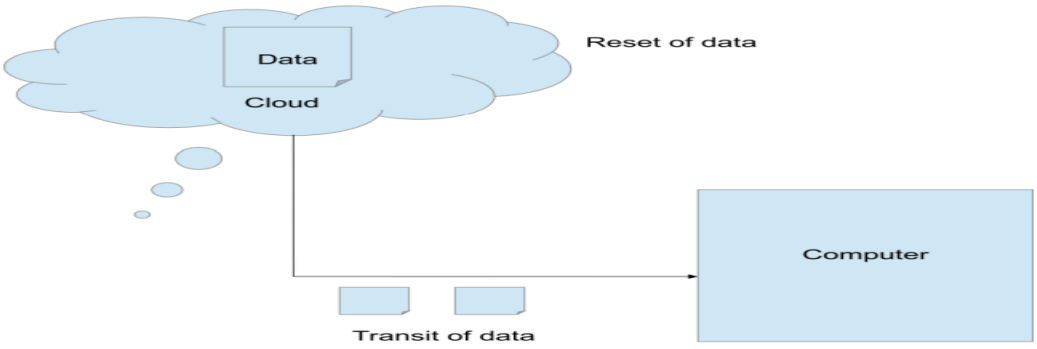


Fig. 3. Data at Reset and transit.

B. Transit of data

The term "data transit" describes the time period during which information is being sent to and from the cloud. Data transit happens when users store their files on the cloud. Therefore, now is a prime opportunity for hackers to steal user information; a system of encryption and decryption is necessary to stop them.

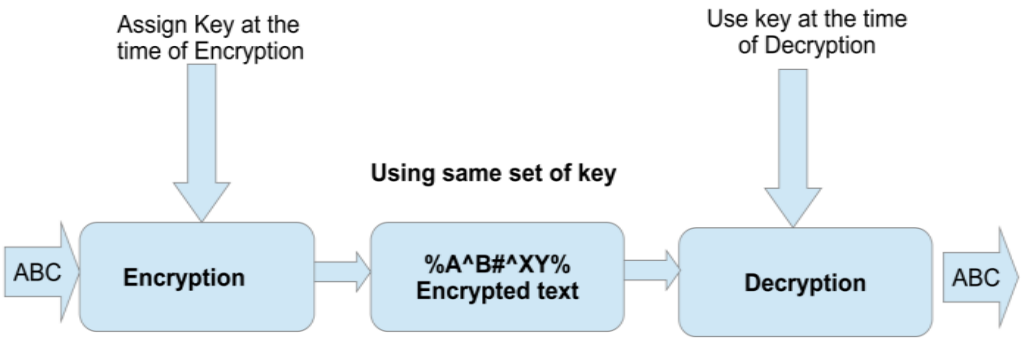


Fig. 4. A Basic Cryptography Approach

ISSN- 2394-5125 VOL 07, ISSUE 01, 2020

In the end, the study's authors decided that asymmetric key encryption was the best method for protecting sensitive information. In this method, the sender and the recipient will each use one of two keys—a private one and a public one—to encrypt and decode the data.

4. PROPOSED METHODLOGY

4.1 Problem Formulation

The safety of data stored in the cloud is the most important factor to consider. There are a number of internal and external attacks that can either wipe the data or expose the most crucial details. Increased system criticality results from the network's representation of data storage as a critical resource. The more the network's accessibility, the greater the opportunity for intrusion. The security of the Cloud System can be compromised by a variety of methods, and a number of different types of data theft can take place in the Cloud. Security issues at the server level, user level, administrator level, data level, and network level are major obstacles in the Cloud. Providing safe and dependable data storage and communication in a Cloud setting calls for a robust security infrastructure. We found one such technology that offers a comprehensive fix for Cloud security problems.

4.2 Algorithm for (LB) Load Balancing

Cloud computing has quickly become the method of choice, with many people now taking advantage of this service. It's adaptable and simple to use, which is why it's so popular. The widespread adoption of cloud computing reflects the growing importance of expanding businesses' ability to serve clients in all regions. The performance parameters of this have also been increasing, thus it has been used. Data stored on the cloud, whether it be public, private, or a hybrid model, will be guarded with a high degree of care. The cloud is no longer merely a place to store data; it also plays a crucial role in a wide range of other domains, such as all social networking sites and numerous online programmes. When working in a cloud environment, load balancing plays a vital role since it allows for more efficient use of resources by distributing workloads evenly among nodes. This, in turn, speeds up processing times and reduces the strain on any given node. The developed algorithm is not provided in terms of previous states but is instead developed in light of the current state of affairs. While developing this algorithm, we made sure to take into account things like load assessment, load link, diverse system strength, system action, node-to-node communication, and so on.

Consider the clustered scenario, where there are different tasks

1. In this first example, we'll pretend there are many different files (X1, X2, X3,... XN).

2. split up file X1 into sub-files (x1, x2, x3, xn) based on when it arrived.

3. the data is parsed into smaller pieces based on the timestamps of the files' arrival.

4. Each partition consists of the same number of sectors (identical in size; let's use 500KB as a minimum).

5. Table 1 below displays the current state of the file chunks:

ISSN- 2394-5125 VOL 07, ISSUE 01, 2020

Table 1 Status of chunks made for each file

File	File Size	No of Chunks (File Size/Threshold size)
X_1	1000 KB	2
X_2	500 KB	1
X_3	2000 KB	4
Total	3500 KB	7

6. Consider the scenario below with 3 servers:

i. Chunk x1 of file X1 is allocated to server S1 and chunk x2 is allocated to server S2.

ii. Chunk x1 of file X2 is allocated to server S2.

iii. Chunk x1, x2, x3 and x4 of file X3 is allocated to S2, S3, S2, and S1 respectively

4.3 Architecture of Proposed Method

The proposed method is illustrated here by its graphical representation. To be more efficient, reliable, and secure than the current method, this one takes a number of files as input and progressively applies defined modules.

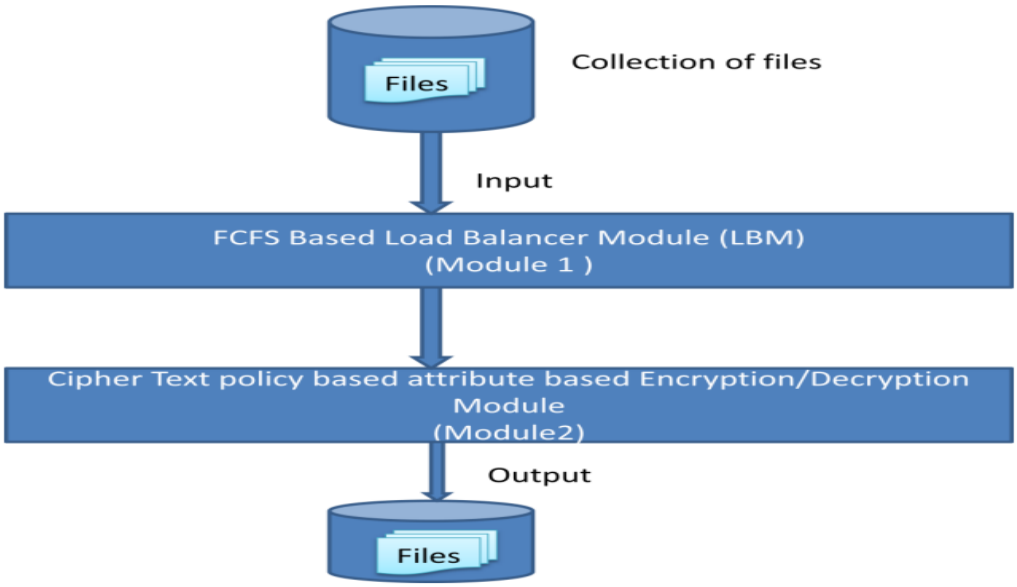


Fig. 5 Complete Architecture of proposed System

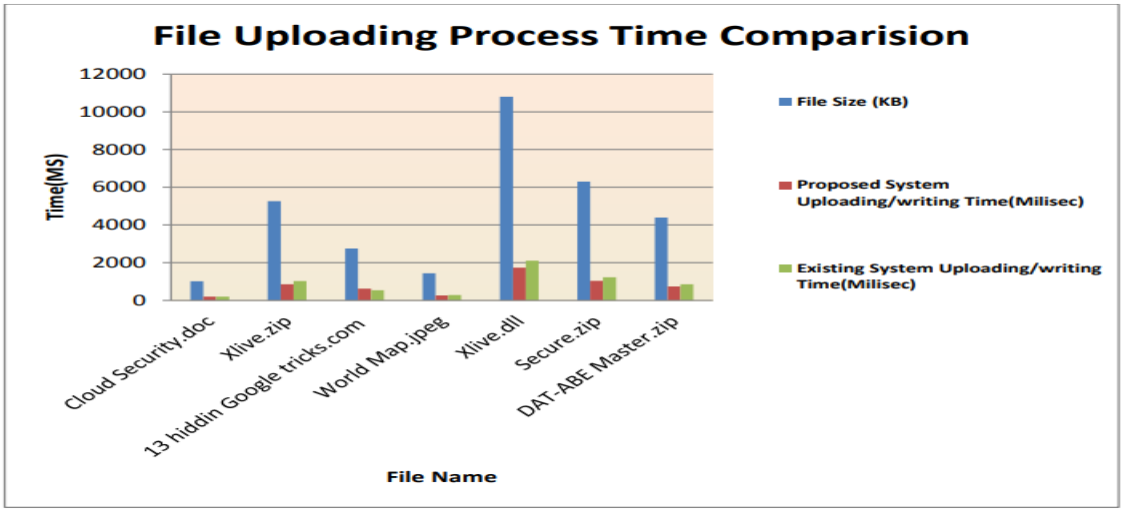
ISSN- 2394-5125 VOL 07, ISSUE 01, 2020

Figure 5 depicts the suggested method's design, which is split into two distinct types:

A. Module 1: FCFS based Load Balancer Module.

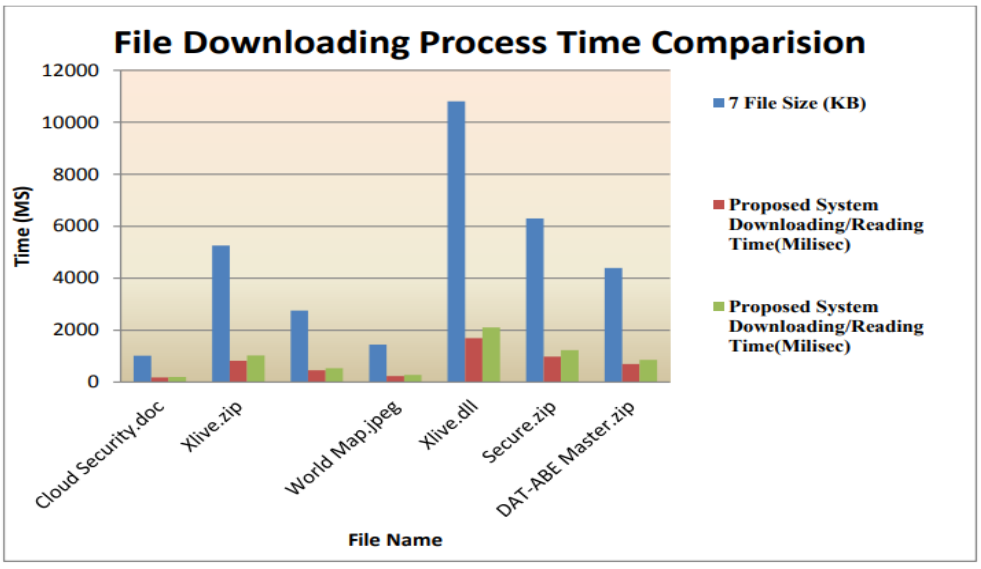
B. Module2: Cipher text attribute based Encryption and Decryption module.

5. RESULTS AND DISCUSSION



Graph 5.1 Result Comparison of File uploading/writing process of different-different files.

Researchers employ a graph comparison method to easily visualise the differences between the proposed and existing methods contained in their respective data sets. This also demonstrates that the proposed solution is faster for huge files than the current methods. Graph 5.1 depicts the approach used to compare the graphs.



Graph 5.2 Result Comparison of File downloading/reading process of different-different files

ISSN- 2394-5125 VOL 07, ISSUE 01, 2020

Researchers employ a graph comparison method to easily visualise the differences between the suggested method and the existing method's files. Similar results are obtained when comparing the suggested solution to the status quo, demonstrating its superiority in terms of download speed for huge files. Also, as can be seen in Graph 5.2, this graphical strategy is put into practise based on the outcomes of seven files of varying sizes.

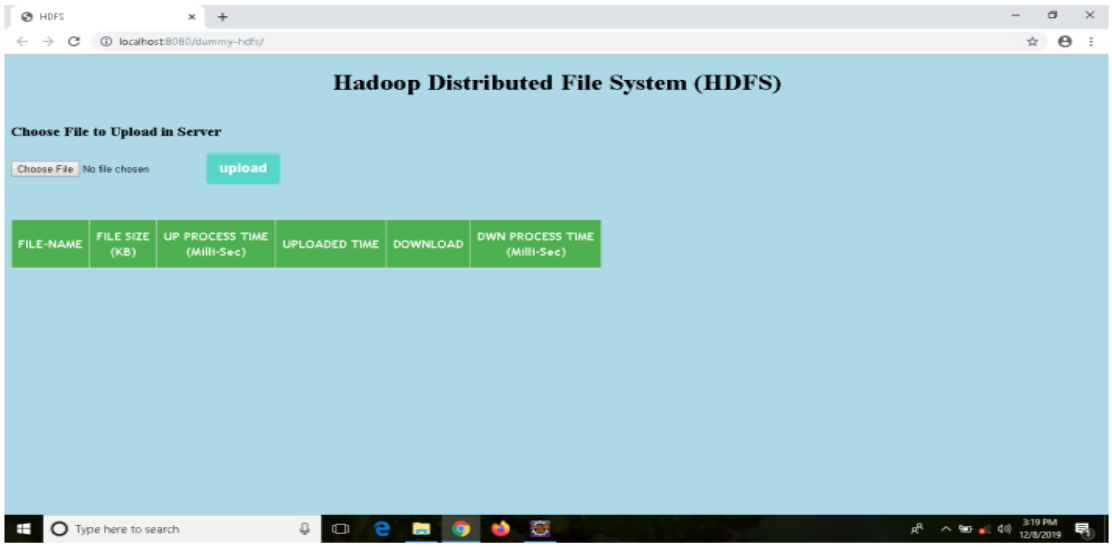


Fig. 5.1 Selection of file for uploading to the server

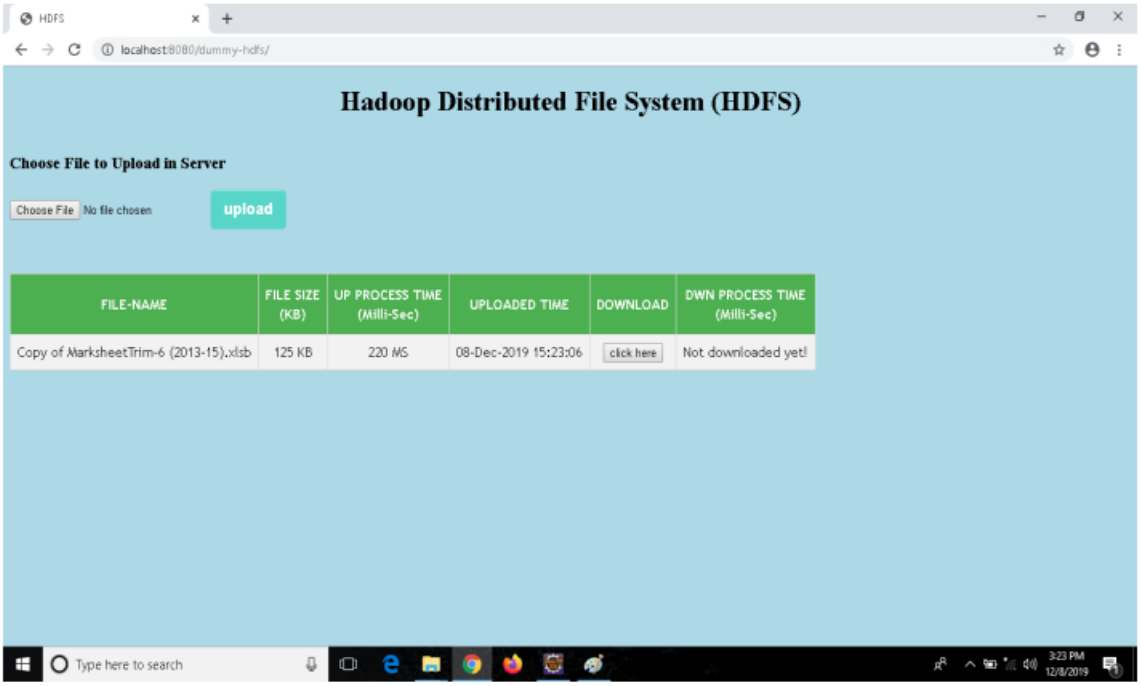


Fig. 5.2 Result of one file after the uploading to the server

ISSN- 2394-5125 VOL 07, ISSUE 01, 2020

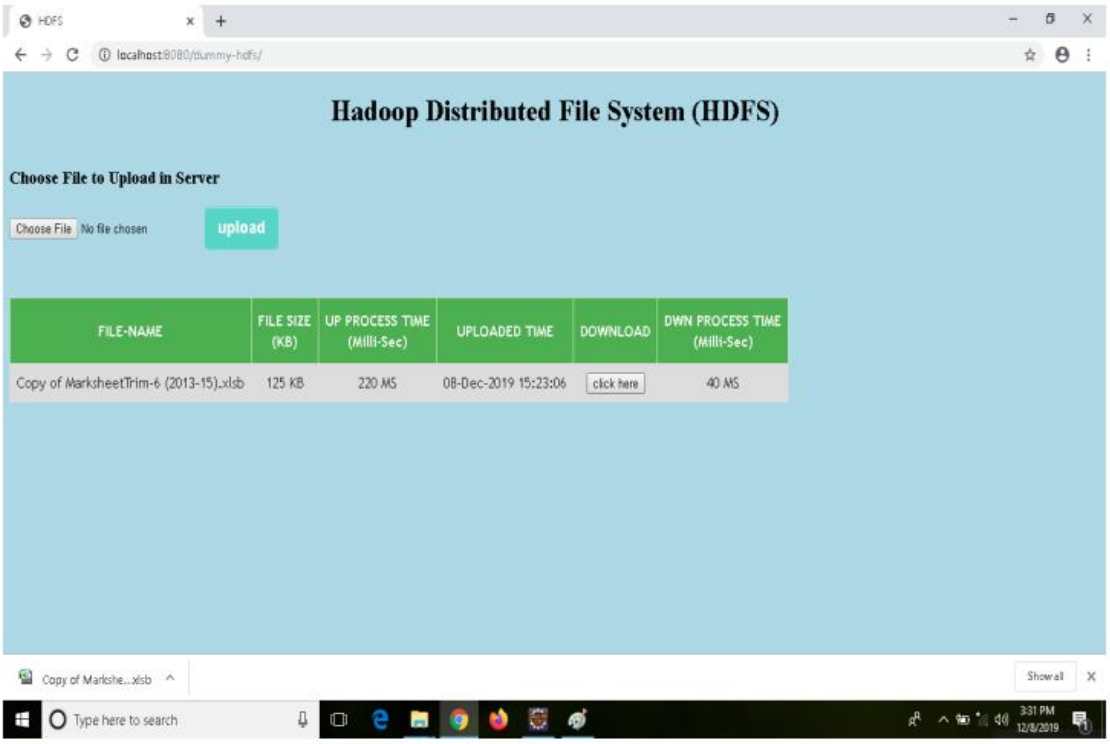


Fig. 5.3 Result of uploading and downloading selected single file to the server.

CONCLUSION

At the conclusion of this paper, the importance of security and privacy has become even more clear to us. Take the lead role in the eyes of your customers. In addition, this has raised people's consciousness about the need to protect the secrecy of their personal records and the significance of those documents in their lives. Various people are still unsure whether they can trust cloud services because of the many pros and cons associated with them. also processing to the cloud. Through the study of security-only problems, privacy-only problems, and interconnected privacy and security challenges, we have considerably advanced our understanding of a wide range of security and privacy issues (vulnerabilities, threats, and assaults). We found and analysed a wide variety of new controls for these issues, which we roughly divided into three groups: controls focused solely on security, controls focused solely on privacy, and controls that combined these two approaches. In addition, the proposed method is more rapid, efficient, and secure than the current method. The proposed method yields variable results depending on the file size, with the fastest speeds achieved for large files when the upload and download rates are both set at 5MB/Sec.

REFERENCES

[1] Wani, A.R., Rana, Q.P., Pandey, N ; Performance evaluation and analysis of advanced symmetric key cryptographic algorithms for cloud computing security ;Advances in Intelligent Systems and Computing, 742, pp. 261-271, 2019 ; DOI: 10.1007/978-981-13-0589-4_24.

[2] Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., Basu, K., Chaudhury, S., Sarkar, P.Cloud computing security challenges & solutions-A survey.2018 IEEE 8th Annual Computing and

Communication Workshop and Conference, CCWC, 2018-January, pp. 347-356, 2018. DOI: 10.1109/CCWC.2018.8301700.

[3] Kaura, W.C.N., Lal, A.Survey paper on cloud computing security ;Proceedings of 2017 International Conference on Innovations in Information, Embedded and Communication Systems, ICIIECS 2017, pp. 1-6, 2018. DOI: 10.1109/ICIIECS.2017.8276134.

[4] Shanmugasundaram, G., Aswini, V., Suganya, G.A comprehensive review on cloud computing security.Proceedings of International Conference on Innovations in Information, pp. 50-71, 2018. DOI: 10.1109/ICIIECS.2017.8275972.

[5] Kaushik, S., Gandhi, C.Cloud computing security: Attacks, threats, risk and solutions (2018) International Journal of Networking and Virtual Organisations, 2018. DOI: 10.1504/IJNVO.2018.093926.

[6] Mehra, N., Aggarwal, S., Shokeen, A., Bura, D. Analyzing cloud computing security issues and challenges Advances in Intelligent Systems and Computing, 710, pp. 193-202,2018. DOI: 10.1007/978-981-10-7871-2_19.

[7] Manoj Kumar, M., Nandakumar, A.N.Exploring multilateral cloud computing security architectural design debt in terms of technical debtSmart Innovation, Systems and Technologies, 78, pp. 567-579, 2018. DOI: 10.1007/978-981-10- 5547-8_59.

[8] Timothy, D.P., Santra, A.K. A hybrid cryptography algorithm for cloud computing security,2017 International Conference on Microelectronic Devices, Circuits and Systems, ICMDCS2017, 2017-January, pp. 1-5, 2017. DOI: 10.1109/ICMDCS.2017.8211728.

[9] Barona, R., Anita, E.A.M. A survey on data breach challenges in cloud computing security: Issues and threats.Proceedings of IEEE International Conference on Circuit, Power and Computing Technologies, ICCPCT 2017. DOI: 10.1109/ICCPCT.2017.8074287.

[10] Sahil, Sood, S.K., Mehmi, S., Dogra, S.Designing and analysis of user profiling system for cloud computing security using fuzzy guided genetic algorithm.Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016, art. no. 7813823, pp. 724-731, 2017. DOI: 10.1109/CCAA.2016.7813823.