CLOUD BASED - DATA STORAGE AND SHARING WITH DUAL ACCESS CONTROL

SK.Yasmin Sulthana[1], B.Kavya Sri[2] ,B.Manasa[3], D.Namrutha[4] S.Chenna Reddy[5]
[1] *Asst. Professor, Krishna Chaitanya Institute of Technology & Sciences , Markapur, A.P, India*
[2,3,4,5] *Scholar, Krishna Chaitanya Institute of Technology & Sciences , Markapur, India*
**E-mail:* yasminbsc6@gmail.com

ABSTRACT:

Due to its effective and affordable administration, cloud-based data storage has recently attracted growing interest from academia and business. Since services are delivered via an open network, it is critical for service providers to adopt secure data storage and sharing mechanisms to protect user privacy and the confidentiality of data. The most popular technique for preventing the compromise of sensitive data is encryption. The actual necessity for data management, however, cannot be fully met by merely encrypting data (for instance, using AES). Additionally, a strong access control over download requests must be taken into account to prevent Economic Denial of Sustainability (EDoS) assaults from being performed to prevent users from using the service.In the context of cloud-based storage, we explore dual access control in this article in the sense that we create a control mechanism over both data access and download requests without sacrificing security and effectiveness. In this article, two dual access control systems are developed, each of which is intended for a different planned environment. There is also a presentation of the systems' experimental and security analyses.

Keywords: Cloud Based Data Sharing, Access Control, Cloud Storage Server, Index SGX, Attribute-Based Encryption.

[1] INTRODUCTION

Utilizing computer resources (hardware and software) that are provided as a service across a network is known as cloud computing (typically the Internet). The term is derived from the widespread usage of a cloud-shaped symbol in system diagrams as a metaphor for the intricate architecture it holds. Cloud computing entrusts the data, software, and processing of a user to remote services. Hardware and software resources are made accessible through the Internet as controlled third-party services in cloud computing. These services typically give users access to cutting-edge server networks and sophisticated software programmes.

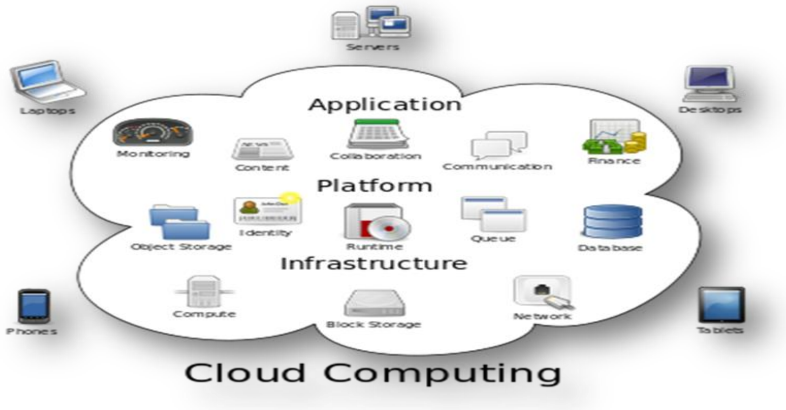

Fig. 1 Structure of cloud computing

Cloud computing aims to apply conventional supercomputing, or high-performance computing power, typically used by armed services and research departments, to perform tens of trillions of computations per second in consumer-oriented applications like financial portfolios, deliver personalised information, provide data storage, or power massively multi-player computer games. Networks of enormous clusters of computers, often running low-cost consumer PC technology with specialised connections, are used in cloud computing to distribute data processing tasks among them. Large networks of interconnected systems make up this common IT infrastructure. The power of cloud computing is frequently maximised by the use of virtualization techniques.

1.2 Characteristics and Services Models:

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

- **On-demand self-service:** A customer may automatically supply computing resources as needed, such as server time and network storage, without needing to deal with the supplier of each service in person.
- **Broad network access:** Capabilities are accessible via the network and used through common methods to encourage adoption by various thin- or thick-client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling:** Using a multi-tenant approach, the provider's computing resources are combined to serve numerous customers, with various physical and virtual resources being dynamically assigned and reassigned in response to customer demand. The consumer typically has no control or knowledge over the precise location of the resources offered, while they might be able to define location at a higher level of abstraction, giving the service a perception of geographical independence.(e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid elasticity:** Capabilities may be provided quickly and elastically, sometimes automatically, to scale out quickly and released quickly to scale in quickly. Consumers frequently perceive the provisioning capabilities as being limitless and able to be ordered in any amount at any time.
- **Metered service:** By utilising a metering capability at an abstraction level suited to the kind of service, cloud systems automatically regulate and optimise resource utilisation (e.g., storage, processing, bandwidth, and active user accounts). The management, control, and reporting of resource utilisation can provide transparency for both the supplier and the consumer.

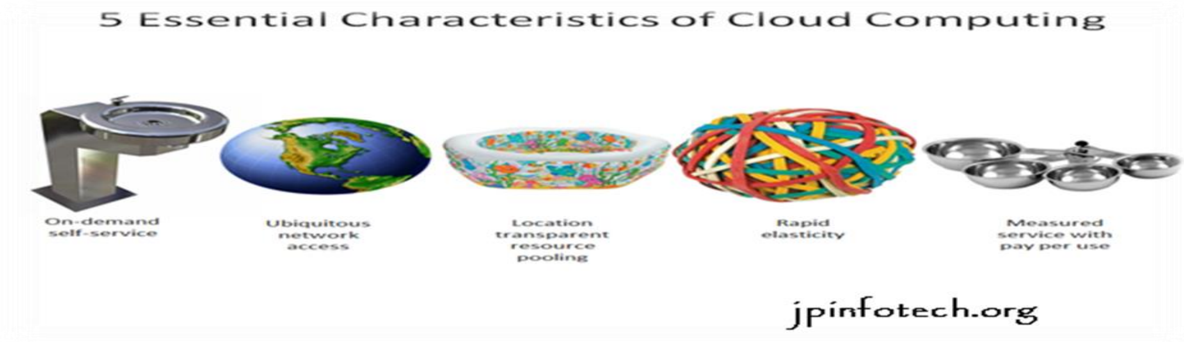

Fig.2 Cloud Computing

1.3 Characteristics of cloud computing

Services Models:

Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service are the three service paradigms that make up cloud computing (SaaS). An end user layer that encompasses the end user perspective on cloud services completes the three service models or layers. The following figure depicts the model. A cloud user can run her own applications on the resources of a cloud infrastructure if she accesses services at the infrastructure layer, for example, and is still in charge of the support, upkeep, and security of these apps. These responsibilities are usually handled by the cloud service provider if she uses a service that is accessible at the application layer.

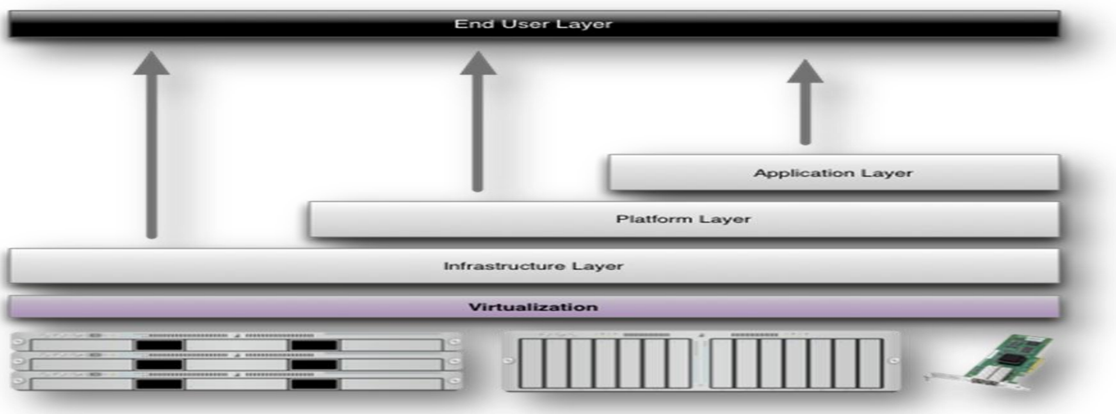

Fig. 3 Structure of service models

1.4 Benefits of cloud computing:

i) **Achieve economies of scale:** Boost productivity or volume production with fewer workers. Your cost per unit, project, or good falls dramatically.

ii) Spend less on technological infrastructure while yet maintaining quick access to your information. Depending on demand, pay as you go (weekly, quarterly, or annually).

iii) **Cheaply and globally expand your workforce:** Anyone with an Internet connection may access the cloud.

iv) Simplify procedures to do more work with less resources.

v) **Lower capital expenses:** You don't need to pay high charges for hardware, software, or licence fees.

vi) **Increased accessibility:** You can access information whenever and wherever you are, which makes life much simpler!

vii) Improve the project monitoring process to stay on budget and ahead of schedule.

viii) Less personnel training is needed:-It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.

ix)**Minimize licensing new software:-**Stretch and grow without the need to buy expensive software licenses or programs.

x)**Improve flexibility:-**You can change direction without serious "people" or "financial" issues at stake.

1.5 Advantages:

a. Cost: Just pay for what you really use.

b. Security: To improve security, cloud instances are isolated from other instances in the network.

c. Performance: For better performance, instances can be added right away. Clients have access to the total resources of the Cloud's core hardware**.**

d. Scalability: Cloud instances may be automatically deployed as needed.

e. **Uptime:** For optimal redundancy, uses many servers. Instances may be automatically produced on a different server in the event of a server failure.

f. Control: Accessible from any place for login. You may deploy unique instances using a software library and a server snapshot.

g. Traffic: Quick deployment of new instances to manage the load is used to address traffic spikes.

[2] LITERATURE SURVEY

The phase of the software development process that is most crucial is the literature review. The time factor, economics, and corporate strength must all be assessed before the tool is developed. Determine which operating system and language may be utilised to construct the tool in the following phases when these conditions have been met. Byzantine et. al., introduced Byzantine Disk Paxos, an asynchronous shared-memory consensus method that makes use of a group of n > 3t discs, of which t may malfunction by being unresponsive or becoming arbitrarily contaminated. We provide two implementations of this approach, i.e., two separate t-tolerant (i.e., tolerating up to t disc failures) building blocks, each of which may be used to solve consensus problems in conjunction with a leader oracle. A t-tolerant wait-free shared safe register is one of the building blocks. The second building piece is a t-tolerant regular register that fulfils a weaker termination (liveness) constraint than wait freedom: although its read operations are guaranteed to return only in executions with a finite number of writes, its write operations are wait-free.With FW terminating registers and a leader oracle, we demonstrate that wait-free consensus may be solved. We refer to this termination condition as finite writes (FW). These ttolerant registers are built from n > 3t base registers, where t may be non-responsive or Byzantine. We are not aware of any earlier FW ending constructions in this model, and all previous t-tolerant wait-free constructions in this model employed at least 4t + 1 fault-prone registers.

Users now frequently utilise consumer cloud storage (CCS) services to store and sync files using apps that are downloaded to their devices. However, the networking performance, service dependability, and data security of a single CCS are intrinsically constrained. We propose UniDrive, a CCS application that integrates many CCSs (multi-cloud) using just a few straightforward public RESTful Web APIs, in order to get around these restrictions. UniDrive has a client-centric, server-less architecture in which all communication is done through file upload and download operations, and synchronisation logic is only performed at client devices. An exclusive distributed lock technique based on quorum ensures strong consistency of the metadata. By carefully dividing erasure-coded data among several CCSs, UniDrive increases dependability and security.UniDrive makes use of all available clouds to optimise parallel transfer chances in order to improve networking performance, but the fundamental idea is the idea of data block over-provisioning and dynamic scheduling. By using a straightforward yet efficient in-channel probing strategy, this group of algorithms hides the complex and variable network characteristics of the underlying clouds and takes use of the quicker clouds more. Numerous test results on the worldwide Amazon EC2 platform and a real-world trial with 272 users demonstrated UniDrive's substantially better and more reliable sync performance than any single CCS.

[3] IMPLEMENTATION AND RESULTS

The paper implementation phase is when the conceptual design is transformed into a functional system. As a result, it may be said to be the stage that will determine if a new system is a success and whether its users have faith in its ability to function well. The implementation step entails meticulous planning, research into the current system and its implementation limitations, creation of transitional techniques, and assessment of transitional methods. The process of putting a new system design into action is called implementation. It is the stage that focuses on site setup, file conversion, and user training in preparation for installing a candidate system. The most crucial aspect here is that the conversion shouldn't interfere with operations of the organization.

The programme is integrated on the Windows 2000 Professional's Internet Information Services 5.0 web server, and it may be accessed from a variety of clients. User capabilities and user training are the two main topics of examination, the system's nature. Users can range from the most basic to the most advanced. Therefore, they should receive software usage training. In the case of an interruption brought on by a power outage, the user should take care to ensure that.

[4] SCREENS SHOTS

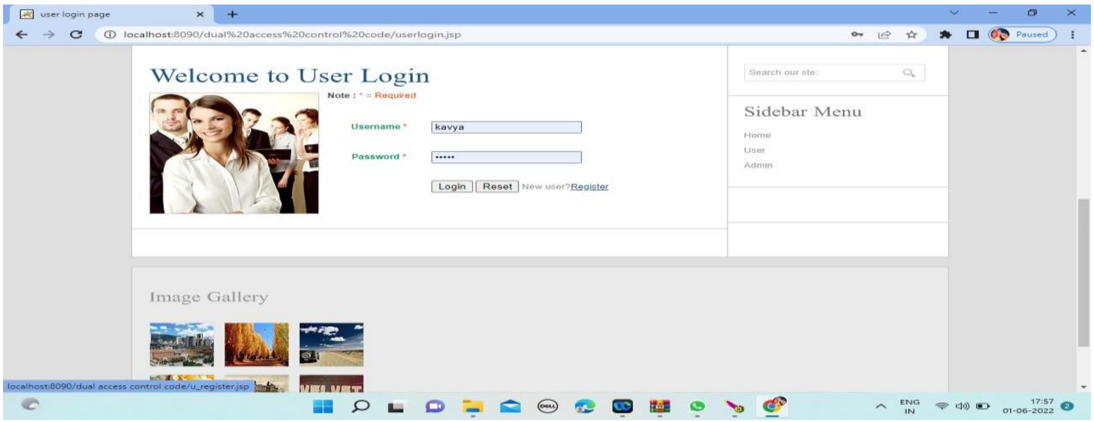

Fig.4 User login

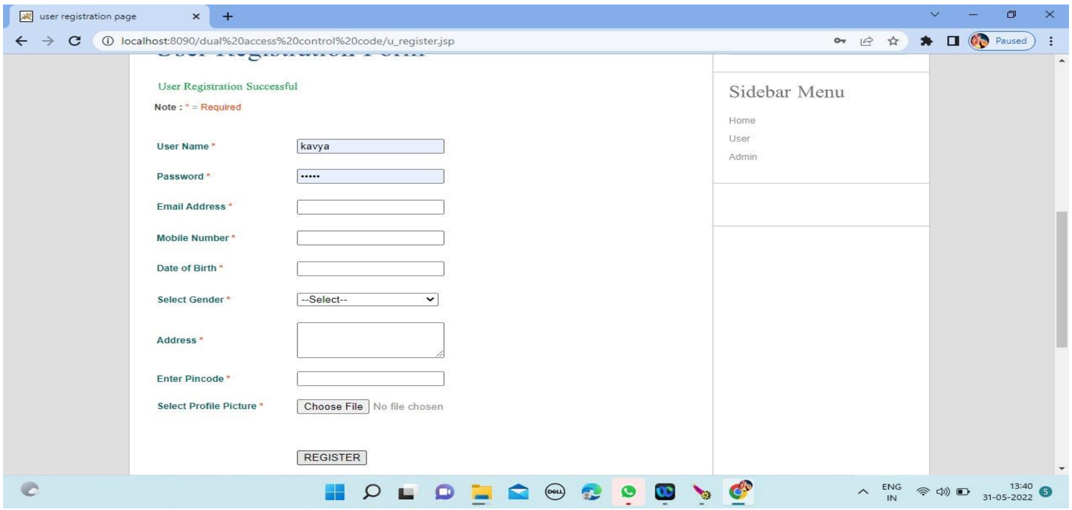

Fig.5 Registration form

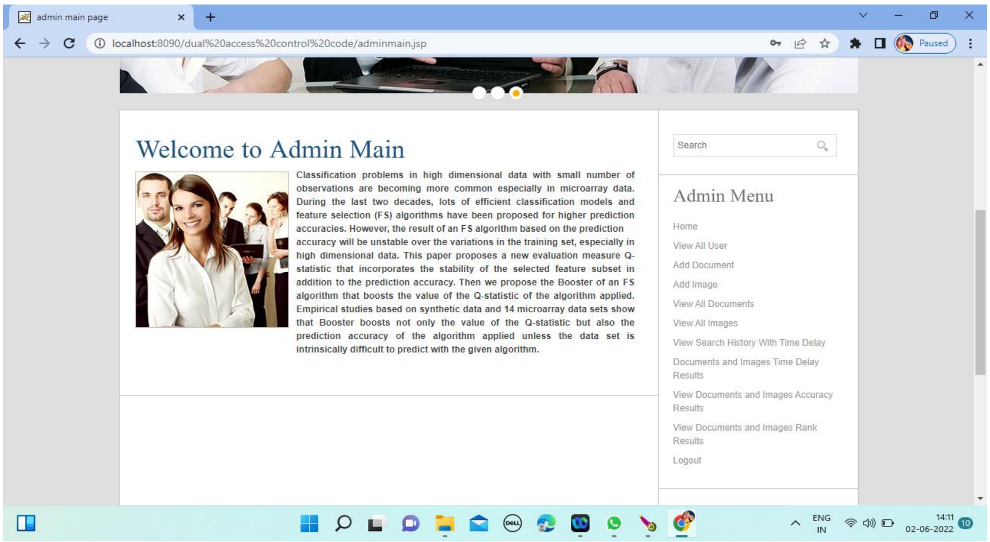

Fig.6 Admin

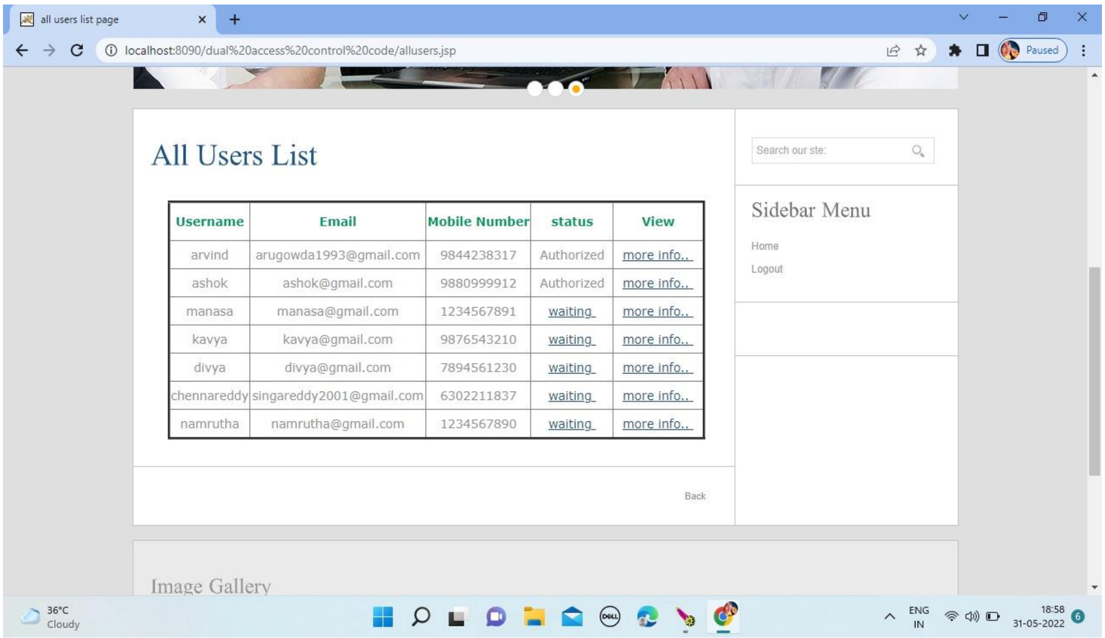

Fig.7 All users

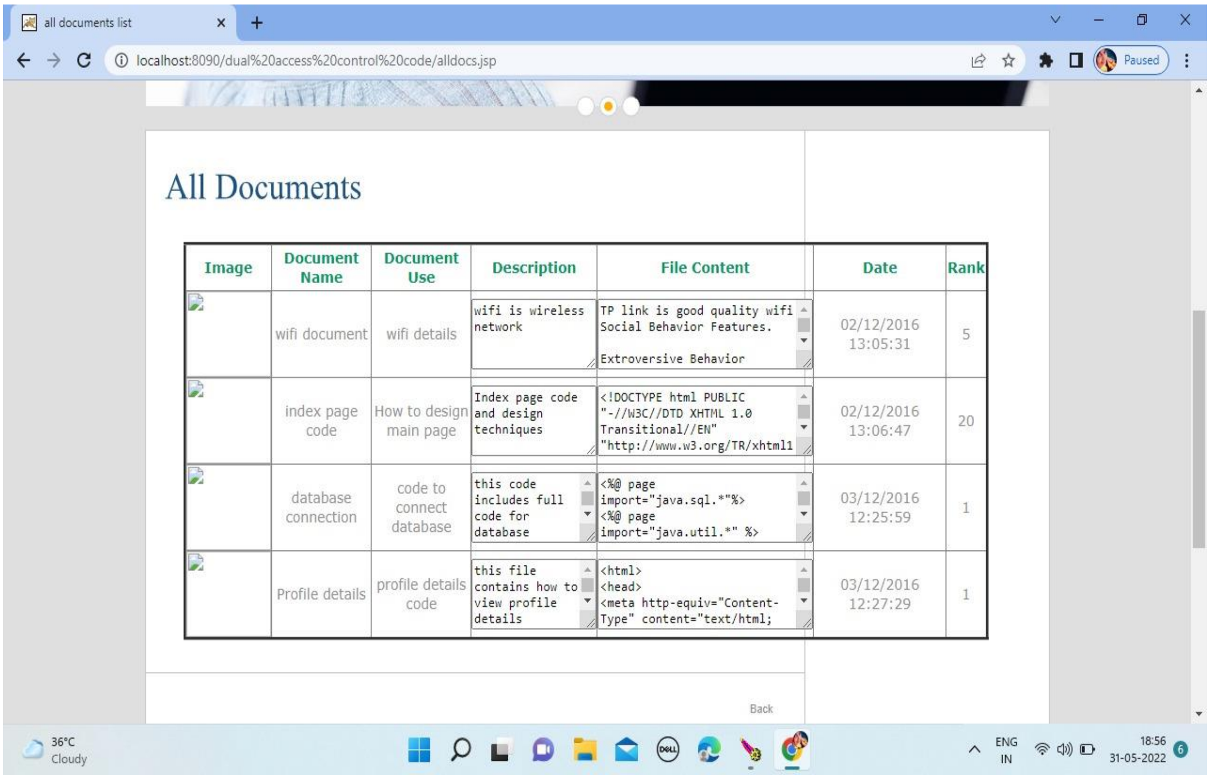

Fig.8 All documents

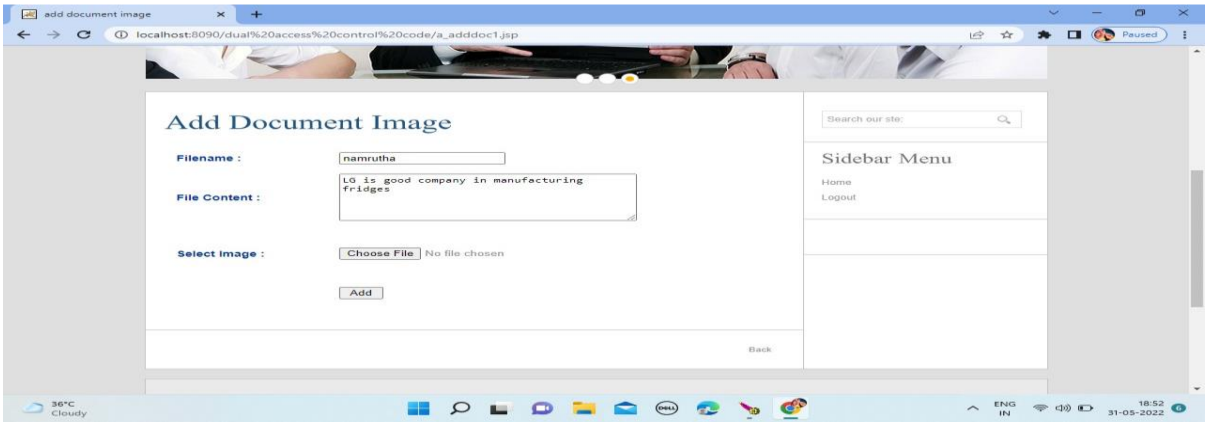

Fig.9 Document image

Fig.10 Time delay

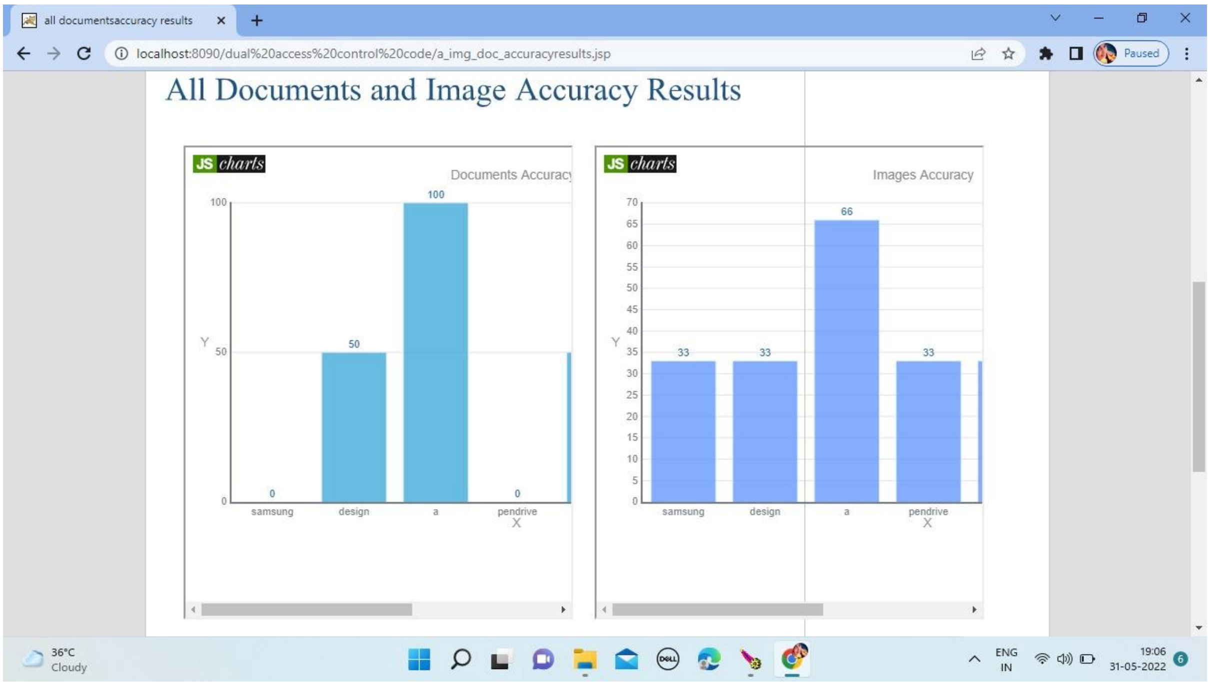

Fig.11 Image accuracy

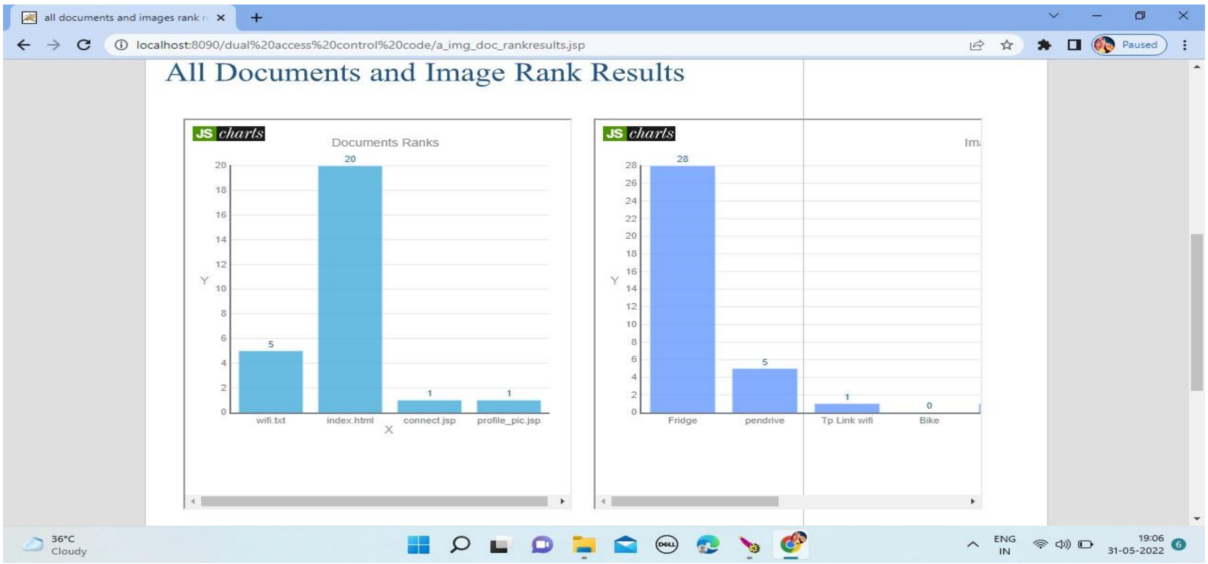

Fig.12 Image rank result

[5] CONCLUSION

We showed two dual access control systems and addressed an intriguing and pervasive issue with cloud-based data sharing. DDoS/EDoS assaults cannot be used against the suggested systems. We claim that different CP-ABE constructions can "transplant" the method utilised to accomplish the feature of control on download request. The proposed solutions don't incur a large computational or communication overhead, according to the findings of our experiments (compared to its underlying CP-ABE building block). We take use of the fact that the secret information entered into the enclave cannot be recovered in our improved system. Recent research, however, demonstrates that an enclave could accidentally reveal some of its secret(s) to a hostile host through memory access patterns or other similar side-channel assaults.Thus, the transparent enclave execution paradigm is shown in. An intriguing challenge is creating a dual access control scheme for cloud data sharing from a transparent enclave. We'll take into account the relevant problem-solving approach in our next work.

REFERENCES

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

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

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

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

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

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

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

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

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

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

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

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

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

[14] Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, Hyesoon Kim, and Marcus Peinado. Inferring fine-grained control flow inside sgx enclaves with branch shadowing. In 26th USENIX Security Symposium, USENIX Security, pages 16–18, 2017.

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

[16] Shaik Abdul Aziz, SK Althaf Hussain Basha, M Narasimha Rao "A Distributed and Collaborative Electricity Consumption and Low Cost Maintenance across Multi Cloud Environment", International Journal For Recent Development In Science And Technology(IJRDST), Volume 04, Issue 07, Jul 2020,pp. 288-293, ISSN:2581–4575.

[17] Mahammad Hafeez, SK Althaf Hussain Basha , N S ,PuttaVenkata Ravi Kumar, "Distributed Approach for Detecting Spammer Across Twitter Through Clustering Techniques" , International Journal For Recent Development In Science And Technology(IJRDST), Volume 04, Issue 07, Jul 2020, pp.252-257,ISSN:2581–4575.

[18] M. Harish Babu, Sk. Althaf Hussain Basha , S. Lakshmana Kumar, "An Advanced DES Based Dynamic Encryption Scheme Over Distributed Computing Across Moving Target Defence", International Journal For Recent Development In Science And Technology(IJRDST), Volume 03, Issue 12, Dec 2019, pp. 277-285,ISSN 2581 –4575

[19] SkNikhath, SK. Althaf Husain Basha, P YejdaniKhan . "Safety Fear/Attacks Current in Cloud Environment", Volume 4, Issue 2, November 2019, pp. 324-330, International Journal of Recent Issues on Computer Science & Electronics(IJRICSE)

[20] Ch. Sowmya, SK Althaf Hussain Basha, , P Yasdhani Khan, "Primary Set and Protection Service IS Transform Data Distribution in Cloud Techniques", Volume 5, Issue 1, Jan-Jun 2019, pp.9-12, International Journal of Recent Issues on Computer Science and Electronics(IJRICSE).

[21] SK Althaf Hussain Basha, Shaik Yasmin Sulthana, "IOT Based Shutter Alarm Security System" Journal of

Engineering Sciences (JES), Vol.11, Issue 7,July/2020, pp.1035-1045, ISSN No:0377-9254.