

B.M.S. COLLEGE OF ENGINEERING

**(Autonomous Institute, Affiliated to VTU)
Bull Temple Road, Basavanagudi, Bangalore - 560019**



A report on

Technical Seminar

“IMPLEMENTATION OF PRIVACY PRESERVATION IN PUBLIC CLOUD”

Submitted in partial fulfillment of the requirements for the award of degree

BACHELOR OF ENGINEERING

IN

INFORMATION SCIENCE AND ENGINEERING

By

Gagandeep S (1BM18IS035)

Deevith H T (1BM18IS031)

Under the guidance of

Chandrakala G Raju
Assistant Professor

**Department of Information Science and Engineering
2021-22**



B.M.S. COLLEGE OF ENGINEERING
(Autonomous Institute, Affiliated to VTU)
Bull Temple Road, Basavanagudi,
Bengaluru – 560019

Department of Information Science and Engineering

C E R T I F I C A T E

This is to certify that the project entitled “**IMPLEMENTATION OF PRIVACY PRESERVATION IN PUBLIC CLOUD**” is a bona-fide work carried out by **Gagandeep S(1BM18IS035), Deevith H T (1BM18IS031)**, in partial fulfilment for the award of degree of Bachelor of Engineering in **Information Science and Engineering** from **Visvesvaraya Technological University, Belgaum** during the year **2021-2022**. It is certified that all corrections/suggestions indicated for Internal Assessments have been incorporated in the report deposited in the departmental library. The project report has been approved as it satisfies the academic requirements in respect of project work prescribed for the Bachelor of Engineering Degree.

Chandrakala G Raju
Assistant Professor

Dr. P. Jayarekha
Professor and HOD

Dr. S.Muralidhara
Principal

Examiners

Name of the Examiner

Signature of the Examiner

1.

2.

ACKNOWLEDGEMENT

The satisfaction that accompanies the successful completion of this Capstone Project Phase-2 would be incomplete without the mention of the people who made it possible through constant guidance and encouragement.

We would take this opportunity to express our heart-felt gratitude to **Dr. B. S. Ragini Narayan**, Chairperson, Donor Trustee, Member Secretary & Chairperson, BMSET. **Dr. P. Dayananda Pai**, Member Life Trustee, BMSET and **Dr. S. Muralidhara**, Principal, B.M.S. College of Engineering for providing the necessary infrastructure to complete this Capstone Project Phase-2.

We wish to express our deepest gratitude and thanks to **Dr. P. Jayarekha**, Head of the Department, Information Science and Engineering and the Project Coordinator's **Prof. Yogesh N** and **Prof. Harini S** for their constant support.

We wish to express sincere thanks to our guide **Prof. Chandrakala G Raju**, **Assistant Professor**, Department of Information Science and Engineering for helping us throughout and guiding us from time to time.

A warm thanks to all the faculty of Department of Information Science and Engineering, who have helped us with their views and encouraging ideas.

Gagandeep S (1BM18IS035)

Deevith H T (1BM18IS031)

DECLARATION

GAGANDEEP S(1BM18IS035), DEEVITH H T(1BM18IS031) students of B.E. Information Science and Engineering, B.M.S. College of Engineering, Bangalore - 22, hereby declare that the capstone project entitled “**IMPLEMENTATION OF PRIVACY PRESERVATION IN PUBLIC CLOUD**” is an authentic work carried out under the supervision and guidance of, **Prof. Chandrakala G Raju** Assistant Professor ,Department of Information Science and Engineering , B.M.S. College of Engineering, Bangalore. We have not submitted the matter embodied to any other university or institution for the award of any other degree.

Place:

Date:

| Name | USN | Signature |
|-------------|------------|-----------|
| Gagandeep S | 1BM18IS035 | |
| Deevith H T | 1BM18IS031 | |

ABSTARCT

Cloud computing is one of the most promising technologies and its benefits are enormous. The real-world situations where cloud computing is at stake and the ways in which industries have reduced these threats are discussed.

To address the risk of data security in the cloud environment, the ability of users to identify true and false is very important. The biggest problem in cloud computing is related to establishing trust between servers and clients. And any internal access to cloud hosting data from vendor data needs to be considered as unauthorized access. Users do no longer understand where their records is stored and there may be a robust perception that users have lost manage in their information after it has been uploaded to the cloud. To allow customers to govern access to their facts saved within the public cloud, suitable access control policies and tactics are required. Accessibility policies should restrict access to data only to data owners.

TABLE OF CONTENTS

| | |
|-------------------------------------------|------------|
| Acknowledgement | i |
| Abstract | ii |
| Table of Contents | iii |
| 1 INTRODUCTION | 8 |
| 1.1 Overview | 8 |
| 1.2 Motivation | 8 |
| 1.3 Objective | 9 |
| 1.4 Scope | 9 |
| 1.5 Existing System | 10 |
| 1.6 Proposed System | 11 |
| 2 PROBLEM STATEMENT | 12 |
| 2.1 Problem Statement | 12 |
| 2.2 Motivation | 12 |
| 2.3 Objectives | 13 |
| 3 DETAILED SURVEY | 14 |
| 4 SURVEY SUMMARY TABLE | 33 |
| 5 SYSTEM REQUIREMENT SPECIFICATION | 34 |
| 5.1 Functional Requirements | 34 |
| 5.2 Non-functional Requirements | 36 |
| 5.3 Hardware Requirements | 37 |
| 5.4 Software Requirements | 37 |

| | | |
|------------|-------------------------------------------|-----------|
| 6 | SYSTEM DESIGN | 38 |
| 6.1 | System Design | 38 |
| 6.1.1 | System Architecture | 38 |
| 6.2 | Detailed Design | 39 |
| 6.2.1 | Use Case Diagram | 39 |
| 6.2.2 | Data flow Diagram | 40 |
| 7 | IMPLEMENTATION | 41 |
| 8 | RESULTS (SNAPSHOTS) | 49 |
| 9 | TESTING | 53 |
| | APPLICATIONS | 56 |
| | CONCLUSION AND FUTURE ENHANCEMENTS | 57 |
| | BIBLIOGRAPHY | 58 |
| | APPENDIX A: LIST OF FIGURES | 60 |
| | APPENDIX B: LIST OF TABLES | 61 |

CHAPTER 1

INTRODUCTION

1.1 Overview

Today building different systems requires a variety of factors to adapt to new technologies. So using a new concept over the clouds has become a daily occurrence. Otherwise, they need better security features to prevent unauthorized access to the system. To do so we need to develop and implement new authorization methods and features. Therefore, when we build systems, we ensure that they are secure and have strong authoritative layers. The risk of data loading with a cloud vendor is likely to be misused in the hosting environment as server control rests with the cloud vendor. This is a major area of concern when data is hosted in a cloud environment.

Everyone uses cloud computing in their daily lives in one form or another without realizing it. To ensure the protection of user data over the cloud many developers have come up with authentication systems, with complex structure or low security, such as for attackers to easily access data. Therefore, our goal is to get the API token on the backend of every authorized user and download their requests using the token as a pass key.

1.2 Motivation

Data validation has become one of the key aspects in the present world scenario. Since the use of hardware storage devices have been reduced over the course of time, tech users are now using virtual cloud to store their personal and professional data. Hence, preserving the authenticity and security of the uploaded data has become the major concern. So, it's a necessary feature to have extra security to maintain the confidentiality of the data.

1.3 Objective

- Everyone are using cloud computing in their day to day life in one or the other form without realizing it. To ensure the protection of the user data over the cloud many developers have come up with authentication systems, which has either complex structure or low security, such that the attackers could easily access the data. So, our aim is to obtain a API token from the backend for every authorized user and fetch their requests using the token as the passkey.
- The main goal of any authentication system is to make sure it's a good system that can be applied and used without facing any problems with unauthorized accesses. Besides, to make sure that the system will be acceptable and doing the job very well in the targeted environment it's going to work in. That's possible if the user is satisfied which means the system should fulfill the user's requirements and needs to the fullest.
- On the other hand, it's important to know end-user's opinions for improving the existing system and generate a better version. It helps to enhance the system's performance and focus on the flaws and the strengths that can be the system's interface as a reason for the user to use this exact system.
- It could be also a prove that the system is excellent and can work properly in organization's environment and be a strong defense for the organization against all the unauthorized people or users. Checking the validity also can be done to reach a level where the customer can give the full trust to the system as a software that achieves all the desired goals and objectives.

1.4 Scope

The purpose of cloud-based authentication is to protect companies from hackers trying to steal confidential information. Cloud authentication allows authorized users across networks and continents to securely access information stored in the cloud with authentication provided through cloud-based services.

1.5 Existing System

To protect the data from misuse there are various methods proposed. Methods include the use of cryptography and authorizing the application to be installed on a client device to perform cryptography-related tasks. Other ways to make a smart encryption management framework work etc. however this has significant management problems and user topics.

The system processor plays an important role in encryption and most cloud providers will provide basic encryption for a few web sites such as passwords and account numbers, as data size increases, the encryption process slows down.

Public cloud is formed by one or more data centers often distributed geographically in different locations. Users do not know where their data is stored and there is a strong perception that users have lost control over their data after it is uploaded to the cloud. In order to allow users to control the access to their data stored in a public cloud, suitable access control policies and mechanisms are required. The access policies must restrict data access to only those intended by the data owners.

These policies need to be enforced by the cloud. In many existing cloud storage systems, data owners have to assume that the cloud providers are trusted to prevent unauthorized users from accessing their Data. Other methods to address the issue of secure data storage in the public cloud include role based access control mechanisms. In role-based access control model, roles are mapped to access permissions and users are mapped to appropriate roles.

This approach requires key management overhead every time the data is accessed. Developing proper security approaches for cloud implementation is a challenging task even though we know about many comprehensive analysis of the main threats that hamper the cloud computing on a wide scale and major vendors have already following some security mechanisms proprietary to their organizations, still there is a lot of research scope for identifying and implementing security mechanisms are needed since customer can't believe blindly when keeping sensitive information with third party service provider, the encryption system can effectively protect the data, but traditional encryption technology is one-to-one encryption.

1.6 Proposed Model

The proposed model is to have a separate system called ‘authentication System’ that interfaces the users to the cloud servers. Before the user’s request is forwarded to cloud server the request is verified in authentication system. These connections are forwarded to cloud server further to access the data stored at cloud server. The user connections are tracked and identified as coming from authentication server at cloud server. Methods to perform stamping of user’s requests are provided. The goal is to hide the data from everyone except the genuine user. Even cloud vendor must login through authentication system to access the data. Hence any transaction to process the data from within the cloud environment is an invalid transaction as the transaction is not stamped from authentication server. The role of the authentication system is to stamp the packets with the signature. Any request with this signature is a valid request in cloud environment. Any operation to open the file /perform read operation on database must be stamped from this system, before the data packets reach the cloud hosting environment. This puts the restriction for the unauthorized access to data in cloud environment. Figure-1 shows the proposed authentication mechanism. The process involves reading the user id and password from the user logged in.

CHAPTER 2

PROBLEM STATEMENT

2.1 Problem Statement

Implementing an external authentication software for accessing files uploaded on the public cloud by user. So that nobody including the cloud hosts can access the files without permission.

2.2 Motivation

Data validation has become one of the key aspects in the present world scenario. Since the use of hardware storage devices have been reduced over the course of time, tech users are now using virtual cloud to store their personal and professional data. Hence, preserving the authenticity and security of the uploaded data has become the major concern. So, it's a necessary feature to have extra security to maintain the confidentiality of the data.

2.3 Objective

- Everyone are using cloud computing in their day to day life in one or the other form without realizing it. To ensure the protection of the user data over the cloud many developers have come up with authentication systems, which has either complex structure or low security, such that the attackers could easily access the data. So, our aim is to obtain a API token from the backend for every authorized user and fetch their requests using the token as the passkey.
- The main goal of any authentication system is to make sure it's a good system that can be applied and used without facing any problems with unauthorized accesses. Besides, to make sure that the system will be acceptable and doing the job very well in the targeted environment it's going to work in. That's possible if the user is satisfied which means the system should fulfill the user's requirements and needs to the fullest.
- On the other hand, it's important to know end-user's opinions for improving the existing system and generate a better version. It helps to enhance the system's performance and focus on the flaws and the strengths that can be the system's interface as a reason for the user to use this exact system.
- It could be also a prove that the system is excellent and can work properly in organization's environment and be a strong defense for the organization against all the unauthorized people or users. Checking the validity also can be done to reach a level where the customer can give the full trust to the system as a software that achieves all the desired goals and objectives.

CHAPTER 3

LITERATURE SURVEY

PAPER 1: Traceable Multi-Authority Attribute-based Encryption Scheme for cloud computing (2017)

The issue addressed in this paper is the security issue that exists at the authority center where based on direct confidentiality and virtual signature, a new multi-characteristic encryption system is proposed. In our system, the signature on the person identification is embedded inside the user's personal key. a third party may be able to directly track the identification of the personal key owner based on the leaked personal key, and might check the validity of the consumer's identification publicly. In addition, multidisciplinary institutions jointly generate user privacy, which effectively solves a security problem that exists within the authority. The results of the performance analysis of the storage show that their system is very appropriate for the cloud computing surroundings.

Mixed with virtual signature technology and a consecutive privacy sharing system, they proposed a system-primarily based encryption system with more than one accreditation facilities and a couple of characteristic centers. Their system can resolve privacy key violations and security center security issues. The proposed system has high protection and overall performance storage, and is nicely appropriate for cloud computing.

PAPER 2: A Multilevel Encryption Technique in Cloud Security(2017)

In this paper cloud privateness is one of the pending problems for cloud computing. since every cloud person does no longer have the same requirements concerning cloud privateness. The whole model of delivery services is vulnerable to security assaults through smart humans. Even though the government and large corporations are rapid approaching an encrypted cloud enclosure that offers a wide range of cloud protection algorithms, all of those algorithms provide one-level encryption. To improve the extent of protection we have advanced a high-level safety scheme that is more relaxed than any sort of single level encryption. Specifically their method indicates that simplest legal

customers can get entry to cloud statistics. Their algorithm is rapid and secure on each sides like report download and down load. as the encryption technique is multi-degree so if some information is misplaced it becomes very difficult to remove the encryption information.

Algorithm: File Upload

```

1. Encrypt_File(F)
2. {
3. /* Phase-1: Encryption of plain text
   file(F) into cipher text using AES
   Algorithm*/
4. for b→1 to Fb
5. {
6. b = E(b,k)
7. }
8. call P(Fe)
9. /* ECC algorithm is used to encrypt
   the key*/
10. for k→1 to maxsize_key(k)
11. do
12. {
13. Pk = Ek
14. }
15. call Pk
16. }

```

Fig 3.2.1: File Upload.

Algorithm_file Download:

```

1. Decrypt_File(Fe)
2. {
3. for k→1 to max of size of (Ke)
4. do
5. {
6. k = D(KA)
7. }
8. return(k)
9. /* Decryption of cipher text */
10. for b1→1 to max number of block(Fe)
11. do
12. {
13. b = Dc (k)
14. }
15. return(F)
16. }

```

Fig 3.2.2: File Download.

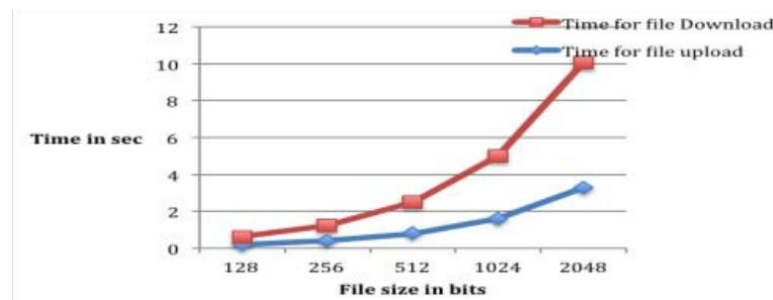


Fig 3.2.3: Runtime of file upload and download in multilevel encryption.

PAPER 3: Cloud Computing Security Threats and Attacks with their Mitigation Techniques(2017)

In this paper based on the principles of computer computing systems, critical computer security requirements, computer protection threats and cloud computing protection attacks with their mitigation techniques, and future studies demanding situations.

however with rapid improvement and attractive donations, the various issues related to this technology also arise which need to be addressed in which safety is the strongest

obstacle to their acceptance. Security issues are an effective research location, which ought to be addressed appropriately to keep away from protection threats and catastrophic attacks on both service companies and service customers.

Discussed on security threats like Data Loss, Data Breaches, Account or Service Hijacking, Insecure Interfaces and APIs, Malicious Insiders, Insufficient Due Diligence, Abusive Use of Cloud Services, Shared Technology Issues, Unknown Risk Profile, Identity Theft, Changes to Business Mode, Lock-IN [3].

A lot studies has been accomplished on cloud security to resolve its problems however due to the rapid increase of this technology security researchers and engineers have no longer been able to offer competitive answers in step with the swiftly growing problems encountered on this region.

PAPER 4: Privacy in cloud computing environments: a survey and research challenges(2017)

In this survey paper the privacy dangers and demanding situations of public cloud computing and efforts to obtain conservation and improve privateness in public cloud.

Different processes are referred to right here as

- (i) data-centric techniques that concentrate on permitting records to guard itself.
- (ii) user-focused approaches that focus on users' involvement in the information protection process through policy explanation, information encryption or records encryption, and many others.,
- (iii) CSP-centric techniques identifying pathways and systems incorporated into cloud infrastructure to make sure privacy.
- (iv) Hybrid techniques related to or greater sorts of strategies.

Several strategies or realistic technique or talent for completing a selected task while an technique is theoretical thoughts/actions/mechanisms supposed to address a problem or situation related to the privateness in the cloud including

Encryption, Processing encrypted data, Obfuscation, Sticky policy, Trusted platform module, Data segmentation, Trusted third party mediator (TPPM) [4].

| Techniques | Strengths | Weakness |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Encryption | Enables strong protection for data at rest Supports any type of data | Data Must be decrypted to be processed Prevent indexing and searching |
| Processing encrypted data | Enables processing the encrypted data Ensures data protection throughout its lifetime Supports any type of data | Adds a high computation overhead Not always feasible in the cloud |
| Obfuscation | Enables to perform sufficient calculation accuracy masked data Provides multiple obfuscation techniques | Weak protection than encryption Not always feasible in the cloud |
| Sticky policy | Sticks data to policy Processing is permitted unless policies are respected | Adds a relatively high overhead Its efficiency depend on the PEP |
| TPM | Provides a shielded location to protect user's data secrets | Cannot perform secure processing Presents a hardware solution |
| Segmentation | Enables protection for data at rest | The loss of a chunk of data leads to the loss of data in all |
| TTPM | Enables a trusted party to check for privacy compliance | Adds high-level computation due to the additional communication traffics |

Fig 3.4.1 : Strengths and weakness of different techniques.

PAPER 5: Survey Paper on cloud computing security(2017)

This is a survey-based paper in which they discuss cloud types and cloud services threats / dangers of computer computing, cloud security guidance, current cloud security system.

The security risks related to cloud computing have to be correctly addressed

- lack of governance
- Obligation ambiguity
- authentication and authorization
- isolation failure
- compliance and legal dangers
- Managing of Protection incidents.
- Control interface vulnerability.
- Software security
- Information protection

There are particularly seven classes of the cloud protection. The issues identified after referring to the diverse references are legal problems, compliance and lack of manage over records.

- Network Protection
- Interfaces
- Information Security
- Virtualization
- Governance
- Legal troubles
- E-Discovery

Cloud generation, diverse security threats and preventative measures to make sure a comfortable cloud system. The need for protection grows and the developing demand for cloud computing services and stability must be stored hand in hand.

PAPER 6: Cloud computing Privacy Issues, Challenges and Solutions(2017)

This paper has addressed and discussed specific security comparisons for Cloud computing, privacy risks and challenges, critical privacy requirements and key types of data.

Understanding the Cloud Data Life Cycle and Privacy Protection Institutions such as T-Clouds Framework, International Telecommunication Union (ITU), International Organization for Standardization (ISO), Cloud Security Alliance (CSA), Organized Information Standards Development (OASIS) [6].

We discussed various computer features and their privateness implications and how appropriate standards and regulations are used to reduce some of the dangers related to hacking client information remotely, and to discuss protection and privacy information for cloud computing.

This paper will recognition on integrating privateness techniques and algorithms right into a cloud computing platform. There's a need to verify the feasibility and power of privateness algorithms and the way it can be incorporated with present cloud computing technology.

PAPER 7: An improved anonymous authentication scheme for distributed mobile cloud computing services(2017)

In this paper cloud computing includes mobile and cloud computing as well as wireless communication technology help to gain the contributors. These contributors consist of mobile customers, mobile provider companies and cloud provider companies. Various demanding situations also exist to enforce mobile cloud computing but protection and privacy are the primary concerns.

There on the way to obtain the security and privateness of the system said by means of the many efforts being made. as the fundamental device is complicated and tends to deal with safety threats, so strong protection and privateness safety schemes are preferred.

Tsai and Lo proposed a verification program based totally on the possession of disbursed cloud computing web sites and claimed that they received a single mark on authentication from more than one provider companies. In addition, they emphasize the significance and safety in their software.

Tsai and Lo scheme are not immune to fraudulent server attacks. It is proven that any enemies with understanding of social barriers can build as a legitimate provider company. An advanced system is then proposed to reduce protection vulnerabilities. the security of the proposed scheme is more desirable below the random oracle version and the tested protocol authentication device prototype ProVerif.

PAPER 8: Ensuring Data Security in Cloud Based Social Networks(2017)

In this paper they stressed that the developers of every day programs have give you new communication websites. consequently, these websites gain greatly by certainly offering a platform for users to connect. It has come to be an integral part of our every day lives, permitting us to talk with our friends and own family on time. because the quantity of social media users grows exponentially, such big data storage is difficult to obtain and

troubles in getting access to facts and privacy of users on cloud-based social media systems maintain. Users are unaware of these problems.

They circulate various photos, motion pictures and personal information on a social community that exists even after deletion. But some of the records disclosed is intended to be confidential, that's why social networking facts has caused the risk of leaking personal information. this is due to the fact they gather a number of private data and customers take the danger of trusting them. As extra private records is shared with the public, concentrated on the privateness of the supposed user will become a great deal less complicated.

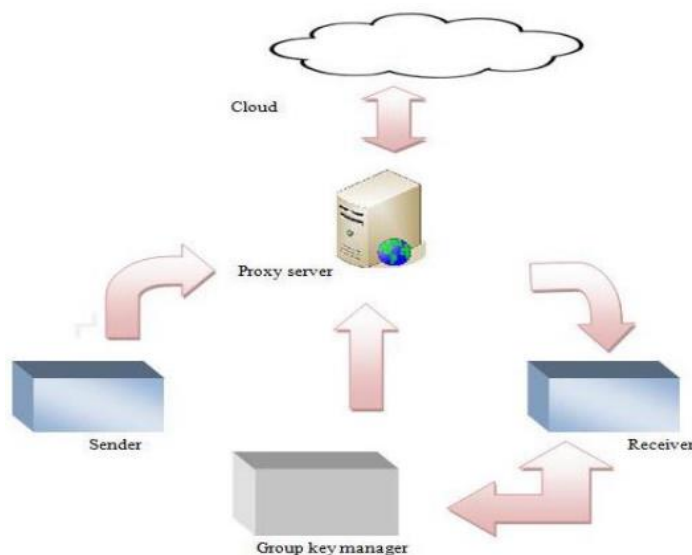
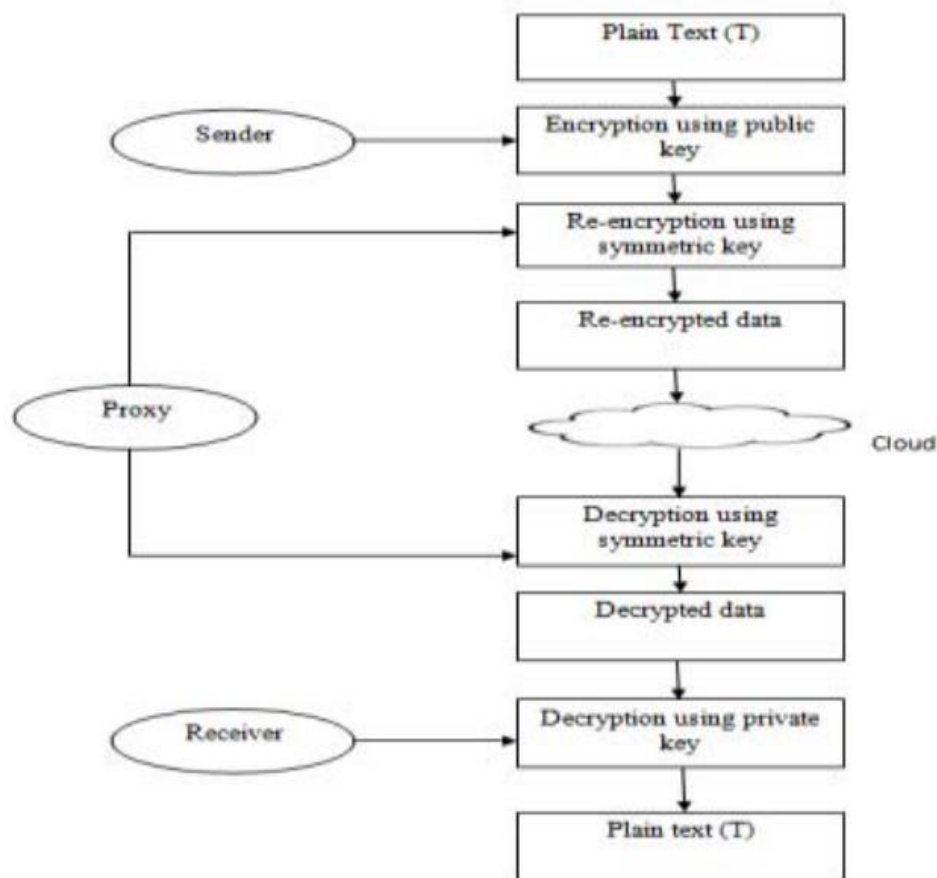


Fig 3.8.1 : Framework outline

Framework for secure information storage on cloud-based totally social networks. The framework encrypts information earlier than storing it within the cloud, and the information is encrypted most effective with the user's personal key, making the records relaxed inside the cloud. Proxy authentication device is used to re-encrypt records to make it greater secure.



PAPER 9: All About Cloud : A Systematic Survey(2018)

This is a survey paper Cloud Computation is a very powerful technology model that can provide very secure data protection and even common storage, so this also prevents various companies from using the cloud to store their data. To provide a better understanding of clouds in terms of their overall characteristics. Private, public and hybrid. Each model has its own features and advantages appropriately, used in conjunction with cloud services - IaaS, PaaS and SaaS computing services.

Cloud Computation is a highly sophisticated technology model that can provide more secure data protection and more common storage, thus further diversifying companies from using the cloud to store their data.

PAPER 10: Review of the Main Security Threats and Challenges in Free-Access Public Cloud Storage Servers(2018)

This paper demonstrates the fundamental assumptions of security inside the adoption of free public cloud storage, but additionally in highlighting approaches to improve export statistics safety.

Major demanding situations Verification, Encryption, Invalid change of assets, Availability, information area, statistics release, Encrypted model manage, established Deletion of records, API Verification, relevant security solutions.

Solutions are offered for challenges such as anonymous verification methods, information sharing, identity tracking strategies, cloud-based space, distance-based totally agreements, client-encryption.

Cloud storage is the best topic because of the increase in the variety of users putting their property at the cloud. But, those customers often do not consider where their information will be stored and who will be able to get entry to this information. It is for this reason that many users feel obligated to use security measures that allows you to have entire control over their statistics. mainly, the person may also experience authentication, integrity, availability, privacy and privacy issues.

Paper 11 : Cloud Computing: Legal and Security Issues(2018)

The paper states that cloud computing is a legal and regulatory challenge. providing a computer agreement for clouds. Cloud Computing provider protection responsibilities and cybercrime. suggested solution protection and data privacy problems. Cloud computing provider companies must protect critical issues related to information privateness. Security and compliance with legal and regulatory functions of cloud computing. Cooperation between service companies, customers and legal entities in all areas and countries is important for achievement.

The big question to be requested is the robustness of Cloud Computing offerings, reliability, availability, and protection essential for clients to go together with this generation? protective customer information from accidental loss or robbery by third

parties is a key driver for Cloud to move ahead and for clients to apply this business model.

Silva proposed a software issue that proved to be effective from checking out with strategies which includes homomorphic encryption and hardware protection extensions the usage of Intel SGX (software security guard Extensions). the first-used Intel SGX in a cloud pc orchestrator produces very low response times and allows for different forms of information calculation, but requires a few infrastructure from the service provider.

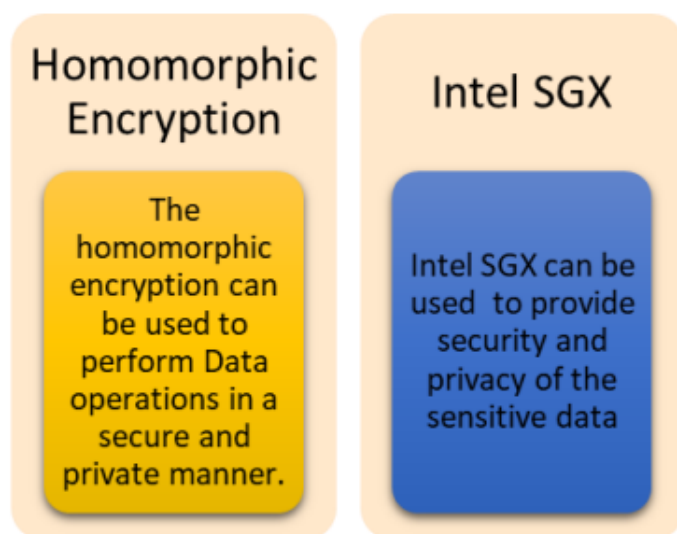


Fig 3.11.1: Combined proposed solution.

PAPER 12: Cloud Computing Security Challenges & Solutions-A Survey(2018)

In this paper various cloud security surveys are already in place, leaving some gap in middle of the appropriate planning of these several problems in their respective results. Various researches introduce Virtualization problems and results while others discuss permission manage measures, lacking is a similar framework that can simultaneously integrate the concept of cloud security with a comprehensive analysis of its specific needs.

Discussions regarding comparisons between cloud data privacy schemes, data integrity, virtualization and its integrity have been discussed. Detailed survey of different perspectives and algorithms used to protect specified sites

In addition, the combat measures given in the research should be visible to indicate the issue being addressed. Having these factors in mind this research paper is organized to manage the required regions with appropriate connections inside them and finally discuss a set of clear issues in this domain.

The paper covers key security holes and protection requirements for a certain cloud system and aims to create an accurate summary of current trends and future prospects for cloud security.

Paper 13: Cloud Security Auditing: Major Approaches and Existing Challenges(2019)

This paper shows why Indigenous Testing is Cloudless and How Cloud Testing Helps Reduce Security Problems.

Discussion on Advanced Protection Features, Non-Medium Log Analysis, Reduced Hand Involvement, Integrated Testing Solution for Multi-Layer Cloud.

First classify the available solutions and specify each category. Second, a taxonomy that identifies categories based on objectives and audit methods. Third, to identify the strengths and weaknesses of these functions. Finally, current challenges in assessing cloud security may draw the attention of security researchers.

They propose a taxonomy that identifies categories based on research objectives and research methods. They also designed the flow of a systematic system of cloud security testing. Also, they do comparative research on existing jobs to see their strengths and weaknesses. Finally, they report the challenges that exist in assessing cloud security.

There are a few limitations of this work that they intend to overcome in our future work. For example, they plan to increase the complexity of the proposed taxonomy in order to more accurately identify gaps in cloud security research. In addition to comparing the quality presented in this paper, they aim to compare existing works in bulk to better understand how to improve the efficiency and accuracy of these methods.

PAPER 14 : Enforcing Confidentiality and Authentication over Public Cloud Using Hybrid Cryptosystems(2019)

A large amount of information is hosted by a cloud-enabled data centre. In Cloud computing, security choices remain the worst case scenario during its development. Specifically in security matters, this study meant coming up with other cryptosystems that are a combination of spick-and-span security measures. The requirement of this test is to protect the data from unauthorized use or from cloud criminals during the communication of encrypted user data. Using public cloud security uses various encryption techniques such as SHA (secure hash algorithms) and blowfish algorithms.

This hybrid cryptosystem is intended to incorporate all the flexible and unequal rules within that blowfish isobilateral law relating to confidentiality of data and, unequal RSA rules come with nursing authorities. This process further includes the Secured Hash-3 rule of data integrity. This standardized method provides maximum security for all network data transfers as well as licensed network access, server, and storage application.

A brief discussion of the various SHA algorithms and their comparisons, and designed for the Encryption System and Definition Process is showed in Fig[3.14.1] and Fig[3.14.2]

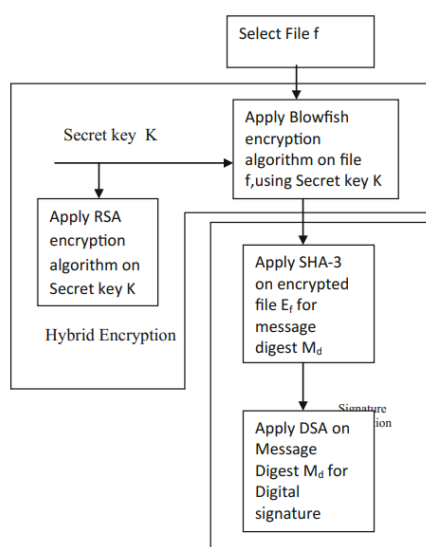


Fig 3.14.1: Encryption process

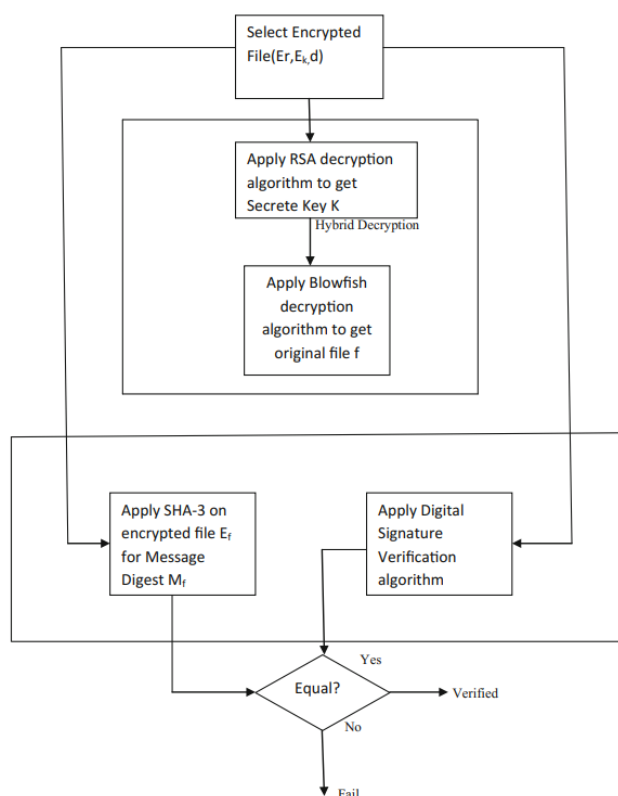


Fig 3.14.2: Decryption process

PAPER 15: A Survey on cloud security issues and block chain(2019)

Cloud computing protection is a primary problem. due to the fact information within the cloud has to be transferred over the internet, data protection becomes a primary challenge. essential approaches to defend information which includes integrity, duty, privacy, access manipulate, authentication, authentication have to be maintained. Blockchain is a generation that makes cloud computing higher. Blockchain overcomes cloud computing protection problems. This examine objectives to analyse and evaluate numerous troubles inside the cloud surroundings with safety problems the use of blockchain. This paper is based on a privacy Survey, keeping records integrity inside the cloud environment and cloud protection issues the use of Blockchain.

Their proposed software is designed for health care systems. All records is transmitted in a file layout within organizations, those documents are encrypted the use of the AES algorithm and integrity is maintained by way of the MD5 or SHA algorithm. The MD5 or SHA algorithm is used to check modifications in statistics saved in cloud storage. a specific user who makes adjustments can be deleted to have comfortable information

switch and cloud storage. similarly Blockchain develops security issues on cloud computing.

Cloud computing is taken into consideration the future of computer technology and storage. activities the use of next-generation technology along with blockchain had been explored on this paper. In considering those security issues we've got advanced a model that complements information integrity. The proliferation of connected gadgets and the growth in computation are a demand for cloud computing inside the current every day trend.

PAPER 16: Cloud Computing Security Challenges and its Potential Solution(2019)

This paper provides current and future trends of this technology, what services the CC offers, security issues and challenges, Attack on Cloud Computing.

Cloud Computing these days is a rapidly evolving and growing technology that is being used in many places now around the world. Provides demand-based computer services and payment for each use of the Internet that accesses a set of shared resources, without having to experience them personally. A key feature of this technology is that the user does not have to worry about any expensive computer infrastructure setting that saves the costs and time of any organization. due to the size and availability of its services. Despite its many advantages, the transformation of a computer system into a virtual computer environment also brings many security challenges and problems for both the consumer and the service provider.

The system maintains data privacy. To gain that kind of trust on a computer, it needs a system that can perform authentication, authentication and encrypted data, so that should keep data privacy.

The best use of the model we need to remove the current security problems on the cloud computing. So in this paper they have used two cryptographic algorithms for RSA and Digital Signature to improve security.

An example of an RSA Digital Signature algorithm is described in specific steps for implementation

1. Suppose John is the sender and Khan is the recipient so the document is taken in the cloud by John and John wants to send that document to Khan.
2. The message will then generate by breaking the document into several lines using a specific Hash function such as (MD5, SHA). used to verify data integrity)
3. John encapsulates message using his secret key. Any effect or generate a digital signature
4. In the final step John uses the RSA algorithm to decrypt a digitally signed signature with a public Khan key and the recipient removes the readable text in a legitimate way by using his private key and verifying the public key signature Khan used.

PAPER 17: Cloud Strike: Chaos Engineering for Security and Resiliency in Cloud Infrastructure (2020)

Many internet attacks and records breaches on cloud infrastructure are because of human mistakes and the risk of malformations. Cloud-focused client equipment are important in lowering these troubles, but present cloud protection models are less likely to deal with those protection challenges.

They propose risk-driven Fault Injection (RDFI) [17] strategies to cope with these challenges. RDFI applies the ideas of turbulent engineering to cloud protection and applies feedback loopholes to provoke, monitor, analyze and prepare security injection campaigns, based totally on expertise base. The information base includes mistakes model models designed from a secure base, superior cloud protection strategies and detection detected in the course of repeated errors injection campaigns. This view allows to identify dangers at the same time as verifying the validity of security features (integrity, confidentiality and availability). in addition, RDFI constantly helps hazard analysis and protection reinforcement efforts via sharing safety statistics and protection measures.

software tool: CloudStrike. numerous experiments had been conducted with CloudStrike towards the infrastructure embedded in the infrastructure of two main public clouds: Amazon web services and Google Cloud Platform. Time performance increases sequentially, in proportion to an growth in attack rates. additionally, the chance evaluation of the error vaccine turned into used to complicate the safety of cloud offerings to reflect the effectiveness of the security information supplied by CloudStrike [17].

PAPER 18: The State of the Public Cloud: Security Concerns with Cloud Computing(2020)

Cloud computing keeps to grow in popularity; but, issues about extended threat for sensitive information maintain to restrict detection. This paper examines the current state of computer protection. It investigates sure protection issues with cloud computing, offers examples of protection threats that preserve to make that problem relevant, and examines the reduction of those threats defined in current literature.

This survey paper examined the many potential dangers related to each of the five cloud protocols. The intention of this paper is to expose how cloud computing gives a promising destiny, however one of the most crucial obstacles to it's far being prevented via issues approximately its protection. specifically, it's far essential that cloud computing companies gather and maintain the believe of their clients, use securely designed system systems, build robust identification control answers, ensure that every customer's software is properly separated from different customers, and comfortable. sensitive information and intellectual belongings of their customers. It describes the effect of these protection risks and their impact at the adoption of cloud computing.

it is possible that extra security of public cloud facts will be of benefit to simplify the safety and manage burden of cloud companies themselves. If cloud computing certainly protects client information security, it will likely be less complicated for cloud companies to make sure that they control this records responsibly.

PAPER 19: Enhancing Public Cloud Security by Developing a Model For User Authentication and Data Integrity Checking (2020)

In this paper an improved model for public cloud user authentication and file integrity testing.

The cloud enforces a few authentication methods so that users can access the files they downloaded, but these methods are not enough as there are cases of file integrity attacks that can be caused by weak authentication systems, weak authentication leads to unauthorized. data access, this is a major threat to user data as a malicious user may gain access to data. In public cloud there is a need for a system that guarantees the integrity of files that may be affected by weak authentication schemes, especially when considering authentication attacks such as session hijackings and intruder attacks.

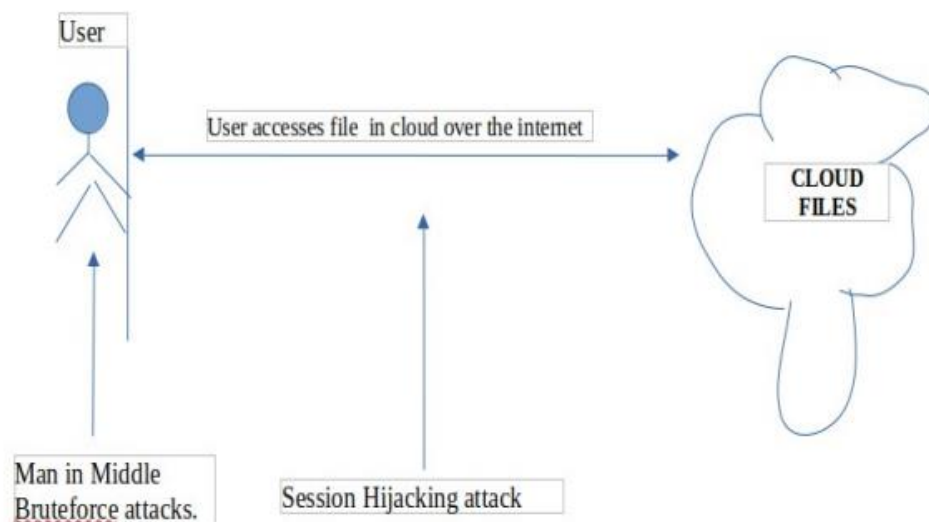


Fig 3.19.1: Description of the problem

The two-factor authentication model uses a username and password as well as a certificate based on user authentication.

To verify authenticity, it uses a two-way method that combines a user's password and digital signature (certification-based authentication), a digital signature is generated from a user program from user data using an RSA cryptography system with a user's

secret key. which is part of his digital certificate, two objects are encrypted using the RSA crypto-system in the user application and sent to the cloud provider.

This proposed model increases user confidence in the cloud application as we use symmetric and asymmetric encryption to upload files to ensure secure communication between cloud users and cloud providers, Model also reduces calculation power on user devices.

PAPER 20: Ensuring user authentication and data integrity in multi-cloud environment(2020)

In this paper there's a need to enhance protection in a cloudy environment which has turn out to be very urgent in latest years. although in this survey, many methods the use of message verification code have been recognized however, the effects of those methods are unsatisfactory and hard to use, which is why the security trouble stays unresolved in this area.

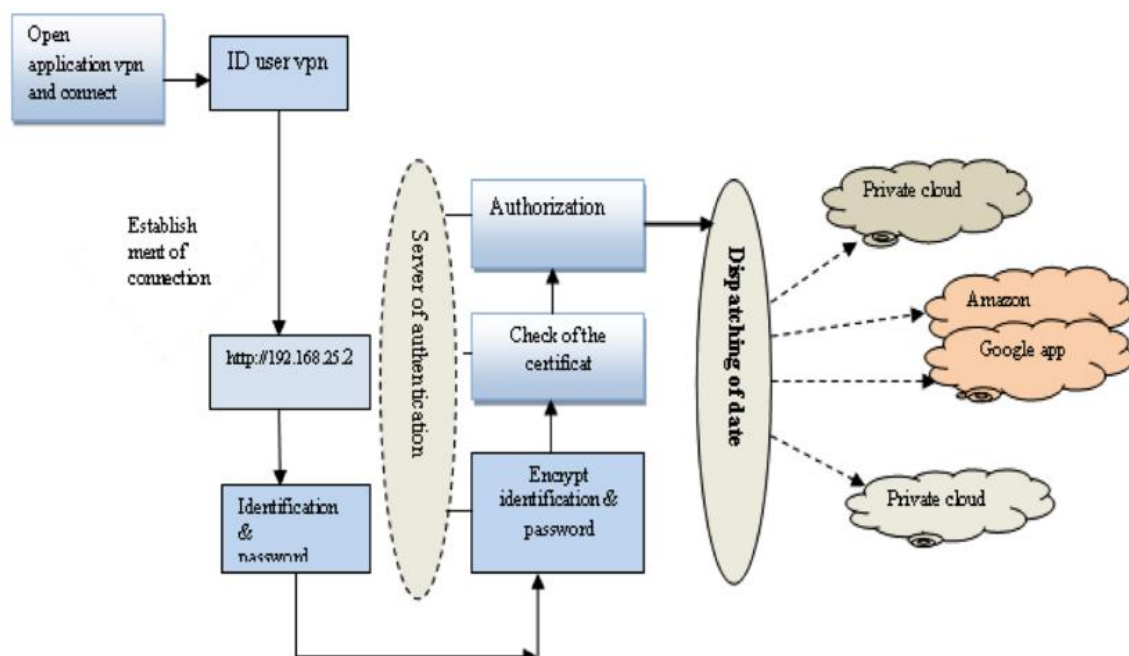


Fig 3.20.1: Overview of model

They suggest a brand new version that offers information validity and integrity in a distributed and usable environment. In this paper, the authors first examine some of the most extensively used protection models inside the region, and then, we introduce a brand new protection approach to this region. Our method consists of three steps, the first step, was to install a personal network to defend the information from the flow. Second, we used an authentication approach based on data encryption, to defend the user's identification and his records, and ultimately, we recognize a set of rules to recognize the integrity of the data disbursed throughout the numerous cloud systems.

The version achieves both ownership authentication and the capability to engage among strategies running on a distinctive cloud company. A records integrity set of rules may be displayed. The outcomes of this proposed version can correctly and effectively build a reliable and strong system within the region of cross-border clouds.

CHAPTER 4

SURVEY SUMMARY TABLE

| SL.NO | Title of the Paper | Problem Addressed | Authors Approach / Method | Results |
|-------|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Traceable Multi-Authority Attribute-based Encryption Scheme for cloud computing (2017) | The security problem existing in an authority center. | linear secret sharing and digital signature, a new multi-authority attribute-based encryption scheme is proposed. | The third party can directly trace the identity of the owner of the private key according to the leaked private key, and can verify the correctness of the user's identity publicly. |
| 2 | A Multilevel Encryption Technique in Cloud Security(2017) | Delivery services model are vulnerable to a range of security attacks by intelligent intruder. Wide range of algorithms provide single level encryption. | To enhance the security level proposed a multilevel security scheme which is more secure than any type of single level encryption. | This technique shows that only authorized user can able to access the cloud data where algorithm is fast and safe in both direction such as upload and download of a file. |
| 3 | Cloud Computing Security Threats and Attacks with their Mitigation Techniques(2017) | Based on cloud computing architectural principles, cloud computing key security requirements, cloud computing security threats and cloud computing security attacks with their mitigation techniques, and future research challenges. | Discussed on security threats like Data Loss , Data Breaches, Account or Service Hijacking, Insecure Interfaces and APIs , Malicious Insiders, Insufficient Due Diligence , Abusive Use of Cloud Services, Shared Technology Issues , Unknown Risk Profile, Identity Theft, Changes to Business Mode, Lock-IN | A lot of research is being conducted on cloud security to resolve its issues but because of the rapid growth in this technology the researchers and security engineers have been unable to provide competitive solutions in accordance with the rapidly growing problems encountered in this area. |

| SL.N O | Title of the Paper | Problem Addressed | Authors Approach / Method | Results |
|-----------|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4 | Privacy in cloud computing environments: a survey and research challenges(2017) | In this survey paper privacy risks and challenges for public cloud computing and efforts to fulfill preserving and enhancing privacy in public cloud. | These approaches are data-centric approaches that focus on how to allow data to protect itself, user-centric approaches, CSP-centric approaches that target mechanisms and hybrid approaches which combine two or more types of approaches. | Several techniques or practical method or skill for completing a specific task while an approach is theoretical ideas/actions/mechanisms intended to deal with a problem or situation related to the privacy in the cloud such as Encryption, Processing encrypted data, Obfuscation, Sticky policy, Trusted platform module, Data segmentation, Trusted third party mediator (TPPM). |
| 5 | Survey Paper on cloud computing security(2017) | | Discussion on types of clouds and cloud services threats/risks of clouds computing, cloud security guidance ,present security system in cloud. | The cloud technology, various security threats and prevention measures for ensuring a secure cloud system. The need for security is increasing along with the increasing demand of cloud computing services and the balance has to be maintained hand-in-hand. |
| 6 | Cloud computing Privacy Issues, Challenges and Solutions(2017) | Cloud computing security incident, privacy risks and challenges, key privacy requirements and critical data types | Understanding the life Cycle of Cloud Data and Privacy Protection Standardized activities like T-Clouds Framework ,International Telecommunication Union (ITU) ,International Organization for Standardization (ISO) ,Cloud Security Alliance (CSA) ,Organization for the Advancement of Structured Information Standards (OASIS). | Discussed the various aspects of computing and its privacy implication and how standards and relevant laws are in place to mitigate some of the risks that are associated of hosting customer data in remote premise, also we mentioned the security and privacy requirements of cloud computing data. |

Implementation of privacy preservation in public cloud

| SL.N O | Title of the Paper | Problem Addressed | Authors Approach / Method | Results |
|-----------|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7 | An improved anonymous authentication scheme for distributed mobile cloud computing services(2017) | In order to achieve security and privacy of the said system several attempts are taken up. As the underlying system is complex and more prone against security threats, therefore strong authentication and privacy preserving schemes are desired. | Identity based authentication scheme for distributed mobile cloud computing environments and claimed to achieve single sign on authentication for multiple service providers. Furthermore, they emphasized the usefulness and security of their scheme. | Then an improved scheme is proposed to mitigate the security weakness. The security of proposed scheme is instantiated under random oracle model as well as the protocol validation model of popular automated tool Pro Verif. |
| 8 | Ensuring Data Security in Cloud Based Social Networks(2017) | the issues in securing the data and privacy of users in cloud-based social networks persist. Users are unaware of these issues. | personalized information is shared with the public, violating the privacy of a target user become much easier. Hence, security of the social networking data stored in the cloud is one of the major issues in cloud-based social networks. | The framework for secure storing of data on the cloud based social networks. The framework encrypts the data before storing it in the cloud, and the data is decrypted only with the private key of the user, making the data secure in the cloud. The proxy re-encryption scheme is used to re-encrypt the data to make it more secure |
| 9 | All About Cloud : A Systematic Survey(2018) | To provide better understanding of cloud in regards with its overall aspects | Private, public and hybrid. Each model has its own characteristics and advantages; accordingly, they are used and cloud computing services-IaaS, PaaS and SaaS. | Cloud Computation is very powerful model in technology which can provide much safer security of data then the traditional storage, so this is also diverting various companies to use cloud for their data storage. |

| SL.N O | Title of the Paper | Problem Addressed | Authors Approach / Method | Results |
|-----------|------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10 | Review of the Main Security Threats and Challenges in Free-Access Public Cloud Storage Servers(2018) | The underlying security assumptions in the adoption of free-access public cloud storage, but also on highlighting the means to enhance the protection of outsourced data. | The main challenges are Authentication, Information Encryption, Inappropriate Modifications of Assets, Availability, Data Location, Data Deduplication, Version control of encrypted data, Assured deletion of data, API's validation, Usable security solutions. | Solutions are given for very challenges such as anonymous authentication mechanisms, data fragmentation, identity traceability mechanisms, Multi-cloud environments, Distance bounding protocols, Client-side encryption. |
| 11 | Cloud Computing: Legal and Security Issues(2018) | Cloud computing legal and regulatory challenges. Cloud computing contractual provisions | Cloud Computing provider's security obligations and cybercrime. A proposed solution for Security and data privacy issues. | Cloud computing services providers must secure the key issues related to data privacy. Security and align with Legal and Regulations aspects of the cloud computing. A collaboration between services provides, customers and Legal bodies in all regions and across countries are essential to succeed. |
| 12 | Cloud Computing Security Challenges & Solutions-A Survey(2018) | Comparison between confidentiality schemes of cloud data , data integrity, virtualization and it's integrity | Detailed survey on the different ideas and algorithms used for the protection of the mentioned areas | The paper covers the essential security loop holes as well as security requirements of an existing cloud system and aims at constructing a proper snapshot of the present scenario and future prospects of cloud security. |

Implementation of privacy preservation in public cloud

| SL.N O | Title of the Paper | Problem Addressed | Authors Approach / Method | Results |
|-----------|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 13 | Cloud Security Auditing: Major Approaches and Existing Challenges(2019) | This paper shows why Traditional Auditing is not Enough for the Cloud and How Cloud Auditing Helps Mitigating Security Issues | Discussion on High-level Security Properties, Non-trivial Log Processing, Reducing Manual Involvement, Unified Auditing Solution for Multi-layer Clouds. | First categorized the existing solutions and elaborate each category. Second, a taxonomy identifying the classifications mainly based on auditing objectives and techniques. Third, to identify the strengths and weaknesses of these works. Finally, current challenges in cloud security auditing which potentially may draw the attention of security researchers. |
| 14 | Enforcing Confidentiality and Authentication over Public Cloud Using Hybrid Cryptosystems(2019) | Implementing security for public cloud using different cryptographic encryption techniques like SHA (secure hash algorithms) and blowfish algorithms | Brief discussion of different SHA algorithms and their comparison, also designed Scheme of Encryption and description Process | The projected methodology defends the client in sequence, starting unconstitutional alright to use throughout the purpose in time of message communication and The finding of study work improves with SHA-3 time unit of improvement has been created. |
| 15 | A Survey on cloud security issues and block chain(2019) | Survey on Privacy, data integrity Preservation in the Cloud environment and cloud security issues using Blockchain | All data are transferred in file format within the groups, those files are encrypted using AES algorithm and integrity is maintained by MD5 or SHA algorithm. The MD5 or SHA algorithm is used to check for the modifications in the data being stored in the cloud storage | Considering the security issues they have proposed a model which increases the integrity of the data. The increase in connected devices and increase in computation is the need for cloud computing in now a-days trend. |

| SL.N O | Title of the Paper | Problem Addressed | Authors Approach / Method | Results |
|-----------|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 16 | Cloud Computing Security Challenges and its Potential Solution(2019) | This paper provide a the current and future trends of this technology, what services provided by the CC, security issues and challenges, Attacks on the Cloud Computing. | The system maintain the confidentiality of the data. To induce that type of trust in cloud computing, there is required a system which can perform verification, authentication and encrypted data transmission, therefore that should maintain the confidentiality of the data. | the best usage of the model we need to remove the current security issues in cloud computing. So in this paper they used two cryptographic algorithms RSA algorithm and Digital Signature in order to enhance the security. |
| 17 | Cloud Strike: Chaos Engineering for Security and Resiliency in Cloud Infrastructure (2020) | Cloud customer-centric tools are imperative for mitigating these issues like human errors and misconfiguration vulnerabilities. | Risk-driven Fault Injection (RDFI) techniques .RDFI applies the principles of chaos engineering to cloud security and leverages feedback loops to execute, monitor, analyze and plan security fault injection campaigns, based on a knowledge-base. | A software tool like Cloud Strike where the analysis of vulnerabilities detected via security fault injection has been used to harden the security of cloud resources to demonstrate the effectiveness of the security information provided by Cloud Strike. |
| 18 | The State of the Public Cloud: Security Concerns with Cloud Computing(2020) | This paper explores the current state of cloud computing security. | This paper approaches security threats that continue to make such concerns relevant, and examines mitigations to these threats described in the current literature. | It explains the impact of these security risks and their impact on the adoption of cloud computing |

| SL.N O | Title of the Paper | Problem Addressed | Authors Approach / Method | Results |
|-----------|------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 19 | Enhancing Public Cloud Security by Developing a Model For User Authentication and Data Integrity Checking (2020) | In this paper an enhanced a model for public cloud user authentication and files integrity checking. | Model that uses the two-factor authentication using the username and password and a certificate based authentication for user authentication. | This proposed model increases user confidence in cloud application as we use symmetric and asymmetric encryption for uploading of files to ensure a secure connection between cloud users and cloud providers, The model also reduces the computation power on user devices. |
| 20 | Ensuring user authentication and data integrity in multi-cloud environment(2020) | Many methods using the message authentication code had been realized but, the results of these methods are unsatisfactory and heavy to apply, which, is why the security problem remains unresolved. | The first step, was to propose a private virtual network to secure the data in transit. Secondly, we used an authentication method based on data encryption, to protect the identity of the user and his data, and finally, we realize an algorithm to know the integrity of data distributed on the various clouds of the system. | The model achieves both identity authentication and the ability to inter-operate between processes running on different cloud's provider. The results of this proposed model can efficiently and safely construct a reliable and stable system in the cross-cloud environment. |

CHAPTER 5

SYSTEM REQUIREMENT SPECIFICATION

5.1 Functional Requirements

- Front end authorizing page – The system shall provide option for the user to login or register for the application. User is required to provide login credentials to login and access the files.
- Backend server to obtain access token – Server shall provide unique access token to each user per session. The access token will be active till the end of session. User should use the same access token to access the files in the cloud.
- External storage to store user credentials – User credentials shall be stored separately in an external storage in an encrypted form.

5.2 Non-Functional Requirements

- User- friendly – User shall be able to use the application easily. Users can easily determine what a feature is and what it can do.
- Security - System typically grants access to account when users enter the correct username and password. Unauthorized access is not allowed into the system. Each user will be provided with unique access token which will expire after each session.
- Compatibility - System allows people who have different operating systems to use the application.
- Reliability – System provides highly reliable functions with the same or similar efficiency after extensive use.

5.4 Hardware Requirements

- Proper internet connection – Internet connection is mandatory for a user to access the system.
- Desktop/Laptop – User must possess a proper working device.

5.4 Software Requirements

- Gitpod.io
- Postman
- React.js
- JWT(JSON web token)

CHAPTER 6

SYSTEM DESIGN

6.1 System Design

6.1.1 System Architecture

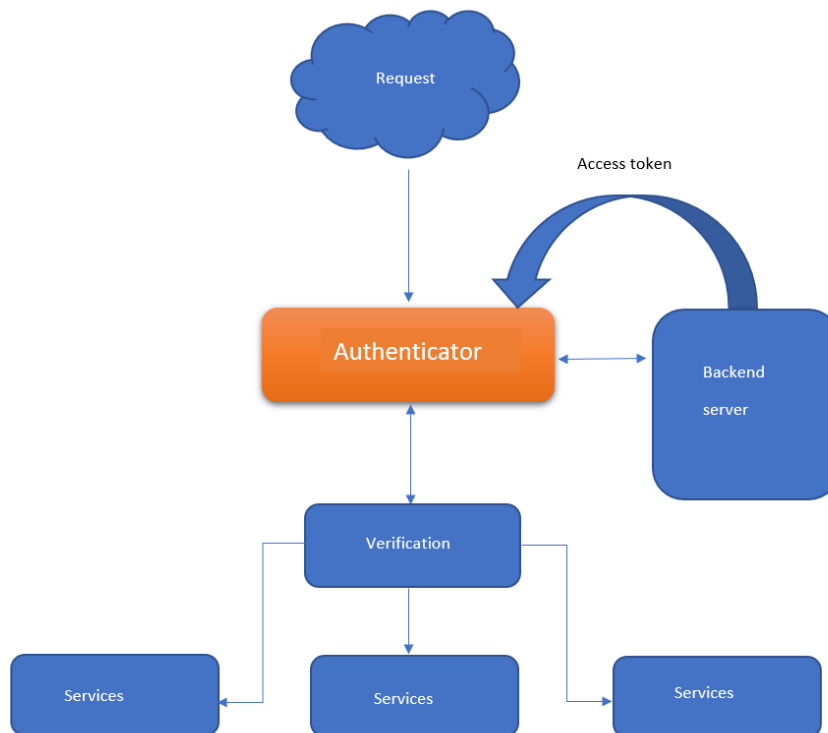


Fig 6.1.1.1: System architecture diagram

- Every cloud user logs into the system.
- And as the authorised person needs to access the files stored in public cloud, he/she is assured the security is their data as we are enabling one more layer of security apart from the one's provided by the hosts of the service.
- The data used for our security model will never be shared with the hosts or any other third parties.
- Once the user verifies his/her credentials with us, they will get the access token which would be the part of the header is every request they make.
- This ensures the total privacy of user data. And allows the user to use all the services without any interruptions or data hindrance.

6.2 Detailed Design

6.2.1 Use Case diagram

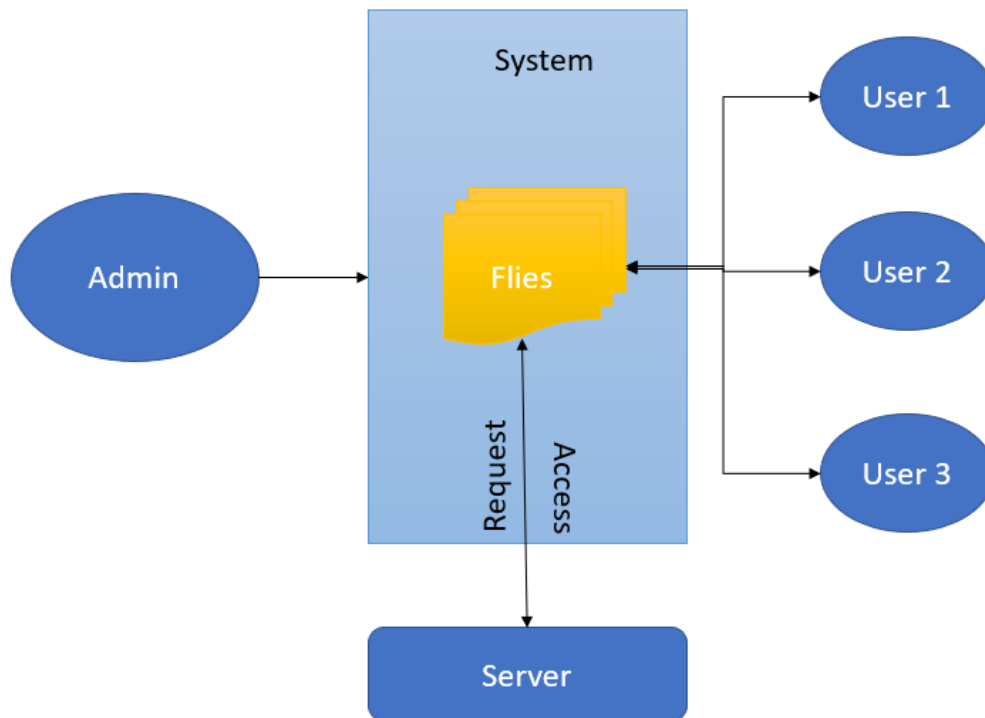


Fig 6.2.1.1: Use case diagram.

Admin – the person who has permission to grant, restrict and remove access for all the clients.

Users – The public cloud users who will be needing the security for all their files over the cloud.

Server - The backend which obtains the token and manages all the requests from user to the server.

6.2.2 Data Flow diagram

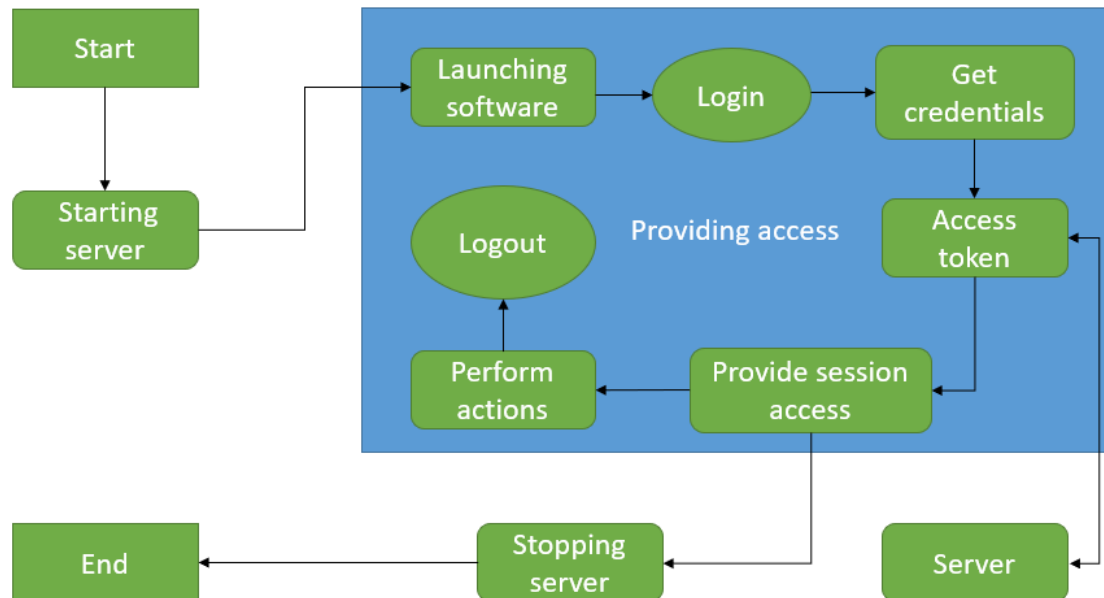


Fig 6.2.2.2: Data flow diagram

Once, the authentication has to begin, API hosts servers are started to launch the software, then the registered user will login to the service by providing the credentials, if the user is verified, the backend server generated a access token for a specific time period, which forms the header of very requests made by the client to the server. Once, the needed actions are performed by the user, they can logout from their account and confirm the extra security provided by this additional layer of authentication.

CHAPTER 7

IMPLEMENTATION

With the objective of increasing the privacy of data over the public cloud, we would wish to implement the extra layer of authentication after the authentication is completed from the cloud host. So, that would be barrier for cloud hosts for accessing the personnel data of the users. For the protection of data from our end, we would not be able pass the layer which the hosts have put in for the users. Hence ensuring the complete security or privacy preservation for the user data.

Here, in this module, explained is setting up of a web application with the help of Python, JavaScript and flask.

Methodology

Considering we have two endpoints or systems that is laptop (client) and a server (api). When a request comes in from the client side that would be an HTTP request from the front end, that request would be answered from the backed server, this communication is stateless, which means that the every new request from the client side , would in a new form without any older knowledge of previous requests. So for every time you do a request from your end you have to tell the backend and verify that the request is from an authorized user. So, we achieve the goal by appending a token as the header of every request we send from our side. Once the server received the request from the user-end, if the user is unauthorized then it will react with the classic 401 (unauthorized), which is the response for unauthorized request. Else if the user does not have access on a particular file, then it would be responded with a 403 (forbidden) error, which is for an authorized user but permission denial service.

If the user request is authorized then the response code would be 200(allowed). Hence a token as the header of each request is necessary.

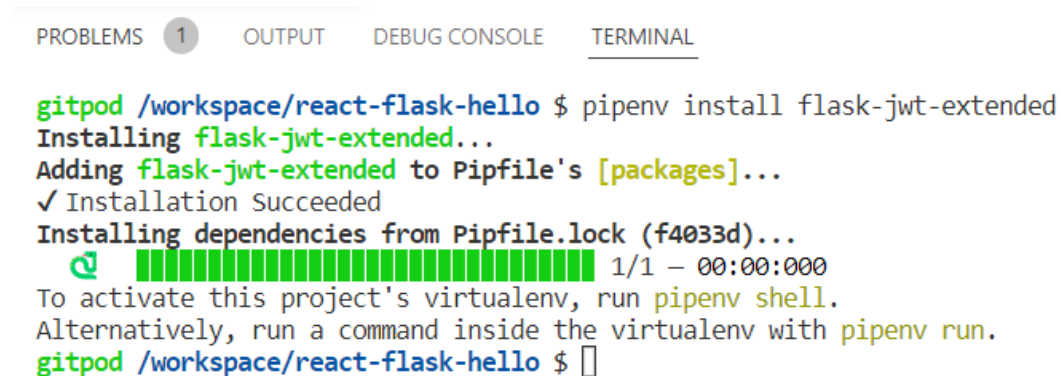
“What is a token?”, It is a random string, which has no meaning but can be used to recognize a particular user.

For an authorized user the steps to be considered are

1. Create token in the backend
2. Storing the token in a session storage for a temporary access
3. Requesting the services with that token

1. Creating a token:

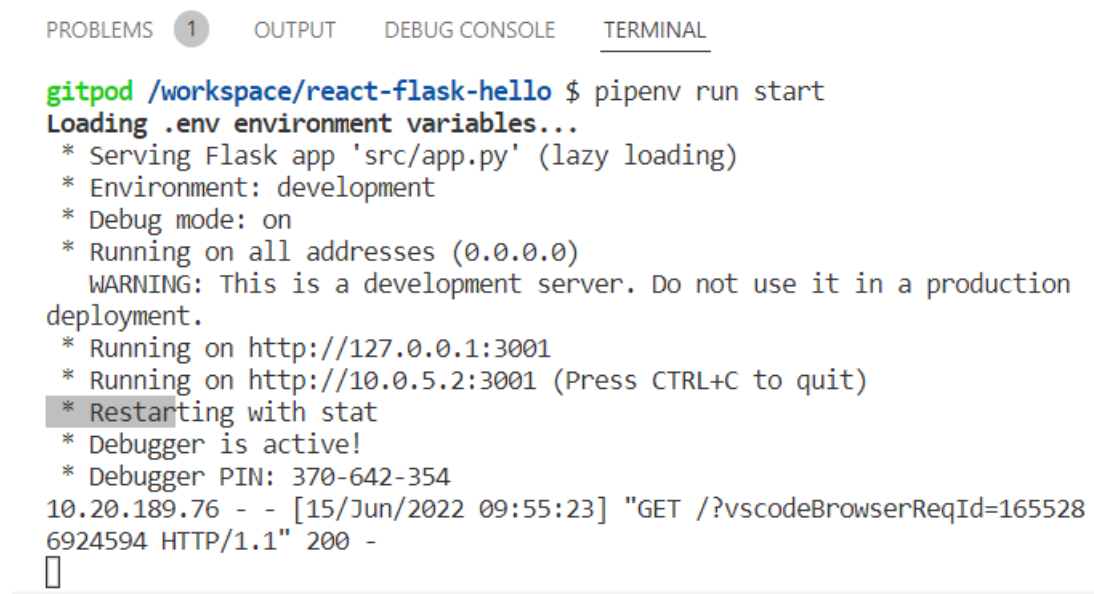
We are using JWT to generate access token, hence we are going to install `Flask_jwt_extended` into our module.



```
gitpod /workspace/react-flask-hello $ pipenv install flask-jwt-extended
Installing flask-jwt-extended...
Adding flask-jwt-extended to Pipfile's [packages]...
✓ Installation Succeeded
Installing dependencies from Pipfile.lock (f4033d)...
  █ 1/1 - 00:00:000
To activate this project's virtualenv, run pipenv shell.
Alternatively, run a command inside the virtualenv with pipenv run.
gitpod /workspace/react-flask-hello $
```

Fig 7.1: Installation of `Flask_jwt_extended`.

Then storing a sample secret key in our backend. For current usage we are using hard-coded username and password, in the future we would be creating user registrations. Now, we need to start the server which would start the local server or the API host on the machine.



```
PROBLEMS 1 OUTPUT DEBUG CONSOLE TERMINAL
gitpod /workspace/react-flask-hello $ pipenv run start
Loading .env environment variables...
* Serving Flask app 'src/app.py' (lazy loading)
* Environment: development
* Debug mode: on
* Running on all addresses (0.0.0.0)
  WARNING: This is a development server. Do not use it in a production
deployment.
* Running on http://127.0.0.1:3001
* Running on http://10.0.5.2:3001 (Press CTRL+C to quit)
* Restarting with stat
* Debugger is active!
* Debugger PIN: 370-642-354
10.20.189.76 - - [15/Jun/2022 09:55:23] "GET /?vscodeBrowserReqId=165528
6924594 HTTP/1.1" 200 -
█
```

Fig 7.2: Starting the server

The below Fig 7.3 demonstrates the launching of the API host from our local server.

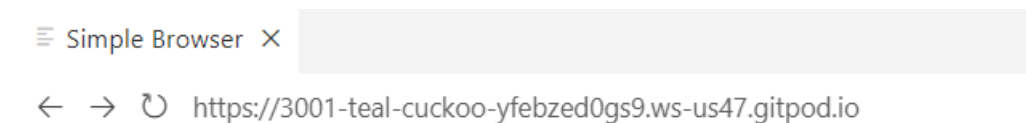


Fig 7.3: API host server

Now, by using postman, and with our API URL generated by the server, create a token by inputting our username and password.

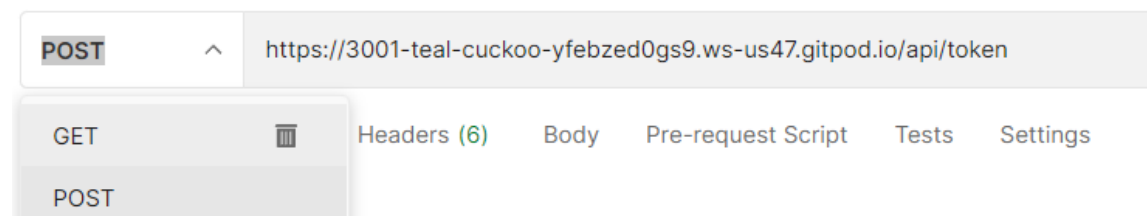


Fig 7.4: Using that URL and POST method.

Implementation of privacy preservation in public cloud

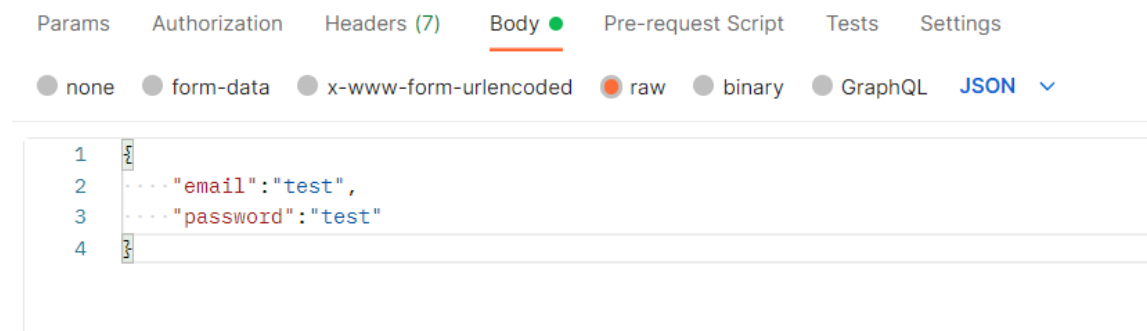


Fig 7.5: Putting JSON code in body .

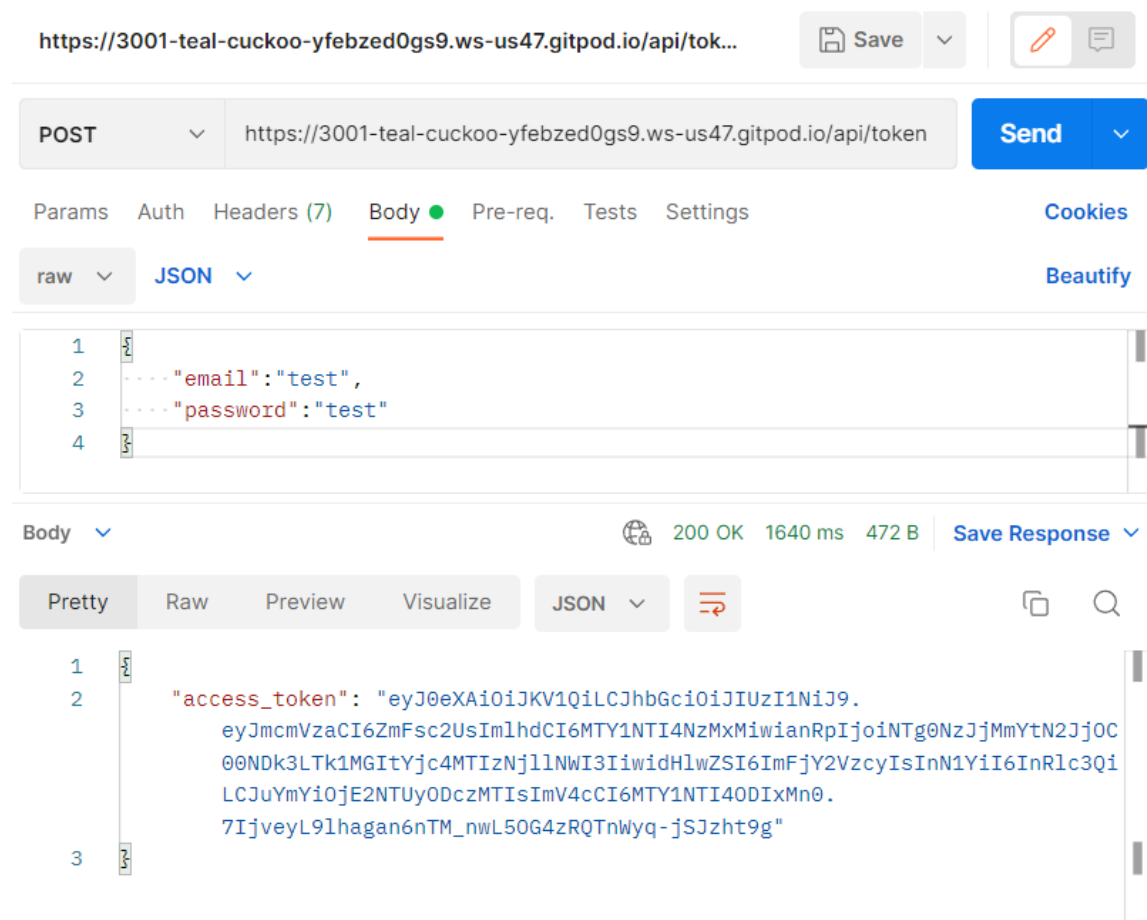


Fig 7.6: Access token generation.

As seen in the above Figures 7.4,7.5,7.6. the access token has been successfully generated.

2. Storing the token

The storage of the access token needs happen in the session storage of the backend, because a newer access token would be generated for the next login of the authorized user.

```
actions: {  
  exampleFunction: () => {  
    getActions().changeColor(0, "green");  
  },  
  
  syncTokenFromSessionStore:()=>{  
    const token=sessionStorage.getItem("token");  
    console.log("Application is loaded, syncing the session storage token");  
    if(token && token!="" && token!==undefined) setStore({token: token});  
  },  
  
  logout:()=>{  
    sessionStorage.removeItem("token");  
    console.log("Logging out");  
    setStore({token: null});  
  },  
  
  login:async(email, password) =>{  
    const opts = {  
      method:'POST',  
      headers:{  
        "Content-Type":"application/json"  
      },  
      body:JSON.stringify(  
        {  
          "email":email,  
          "password":password  
        }  
      )  
    }  
  }  
}
```

Fig 7.7: login and logout actions

The above Fig 7.7, shows the token storage spaces and the actions performed like login and logout from our authenticator.

The below Fig 7.8, represent the token fetch from postman and storing it in the temporary storage.

Implementation of privacy preservation in public cloud

```
//fetching token from the postman
try{
  const resp = await fetch('https://3001-teal-cuckoo-yfebzeds9.ws-us47.gitpod.io/api/token', opts)
  if(resp.status !== 200) {
    alert("errors");
    return false;
  }

  const data=await resp.json();
  console.log("from backend",data);
  sessionStorage.setItem("token",data.access_token);
  setStore({token: data.access_token});
  return true;
}catch(error){
  console.error("there has been an error in login")
}

getMessage: () => {
  const store=getStore();
  const opts={
    headers:{
      "Authorization":"Bearer " + store.token
    }
  };
  // fetching data from the backend
  fetch("https://3001-peach-chicken-r26wzrx0dn6.ws-us47.gitpod.io/api/hello",opts)
    .then(resp => resp.json())
    .then(data => setStore({ message: data.message })))
    .catch(error => console.log("Error loading message from backend", error));
},
```

Fig 7.8: Fetching token from the postman

Once the token is generated for a given user, he can login and perform action as required and logout by removing the presence and might need to login again with a newer access token for next access onto his public cloud.

```
gitpod /workspace/react-flask-hello $ npm run start

> react-hello-webapp@1.0.1 start
> webpack-dev-server --config webpack.dev.js --port 3000

<w> [webpack-dev-server] "hot: true" automatically applies HMR plugin, you don't have to add it manually
to your webpack configuration.
<i> [webpack-dev-server] Project is running at:
<i> [webpack-dev-server] Loopback: http://localhost:3000/
<i> [webpack-dev-server] On Your Network (IPv4): http://10.0.5.2:3000/
<i> [webpack-dev-server] Content not from webpack is served from '/workspace/react-flask-hello/dist' directory
<i> [webpack-dev-server] 404s will fallback to '/index.html'
Browserslist: caniuse-lite is outdated. Please run:
  npx browserslist@latest --update-db
  Why you should do it regularly: https://github.com/browserslist/browserslist#browsers-data-updating
<i> [webpack-dev-middleware] wait until bundle finished: /
asset bundle.js 1.41 MiB [emitted] (name: main) 1 related asset
asset 4geeks.ico 19.3 KiB [emitted]
asset bms_logo.jpg 12.5 KiB [emitted] [from: src/front/img/bms_logo.jpg] (auxiliary name: main)
asset index.html 1.21 KiB [emitted]
runtime modules 26.3 KiB 13 modules
modules by path ./node_modules/ 1.26 MiB 73 modules
modules by path ./src/front/ 25.7 KiB
  modules by path ./src/front/js/ 19.2 KiB
    modules by path ./src/front/js/pages/*.js 6.37 KiB 5 modules
    modules by path ./src/front/js/component/*.js 3.29 KiB 3 modules
    modules by path ./src/front/js/*.js 2.24 KiB 2 modules
    modules by path ./src/front/js/store/*.js 7.34 KiB 2 modules
  modules by path ./src/front/styles/*.css 6.39 KiB
    ./src/front/styles/index.css 2.3 KiB [built] [code generated]
    ./node_modules/css-loader/dist/cjs.js!./src/front/styles/index.css 720 bytes [built] [code generated]
    ./src/front/styles/home.css 2.29 KiB [built] [code generated]
    ./node_modules/css-loader/dist/cjs.js!./src/front/styles/home.css 1.1 KiB [built] [code generated]
    ./src/front/img/bms_logo.jpg 56 bytes [built] [code generated]
webpack 5.65.0 compiled successfully in 5434 ms
```

Fig 7.9: Starting webpage.

FACE API INCLUSION

We would like to include a biometric verification for our authenticator and generate a new token, which would be aggregated with the previously obtained token and increase the security over the cloud.

Here, we have used an open source face API namely Compreface which provides the service of face verification.

Exadel CompreFace is a free and open-source face api service that can be easily integrated into any system. CompreFace provides REST API for face recognition, face verification, face detection is easily deployed with docker.

CompreFace is delivered as a docker-compose config and supports different models that work on CPU and GPU. Our solution is based on state-of-the-art methods and libraries like FaceNet and InsightFace.

They claim an accuracy of about 99.8% over LFW dataset.

Steps For Implementing Compreface

Initially, we need to set up docker desktop on our service and obtain the compreface archive provided by them. Then run the docker command to start the service and launch the application over the localhost on our system.

Compreface provides a basic sdk which is shown in the Fig 7.10 below.

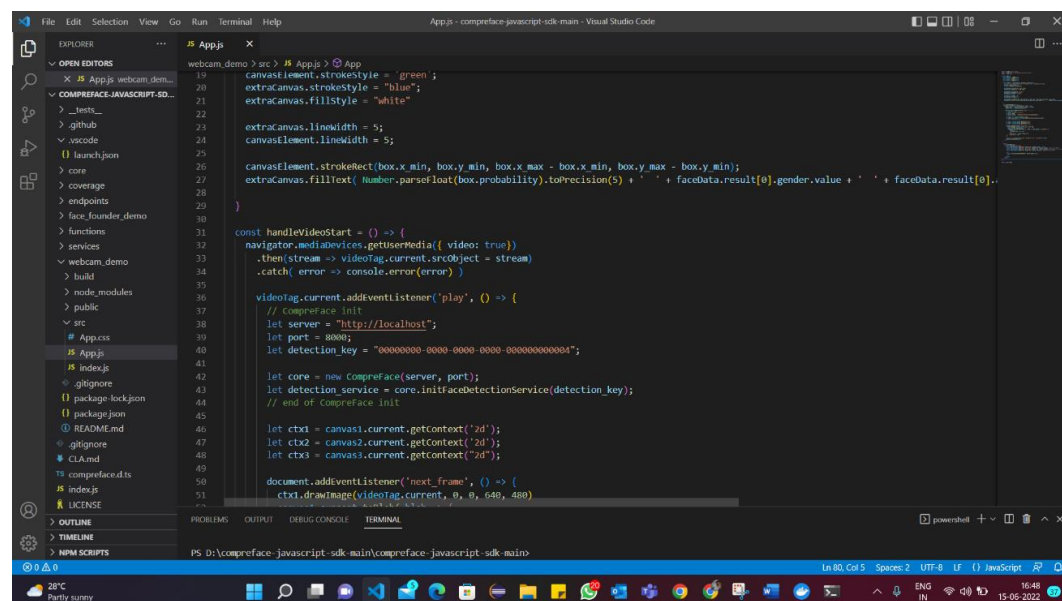


Fig 7.10: code snippet of CompreFace

The admin will have to setup up his account and receive the api token to the sample sdk.

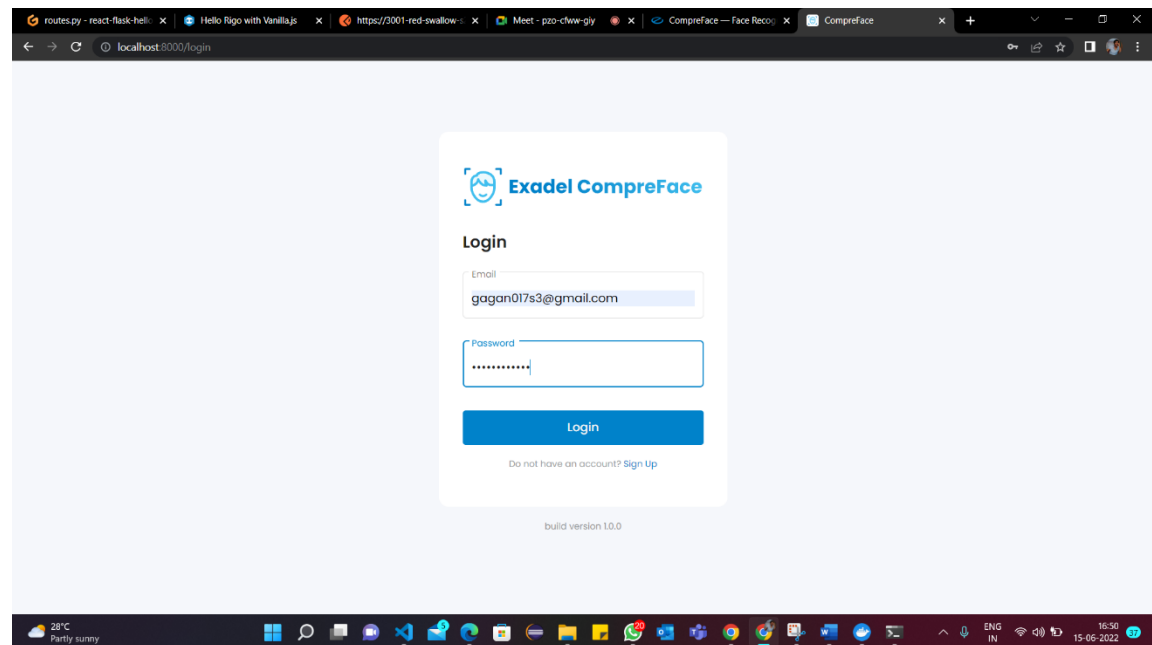


Fig 7.11 : login in and sign in page for compreface

Later on, the face stored in while registering an user will be used to again verify him and obtain a access token if the similarity index is more than 0.95. This token will be concatenated with the one which will be obtained from username and password previously.

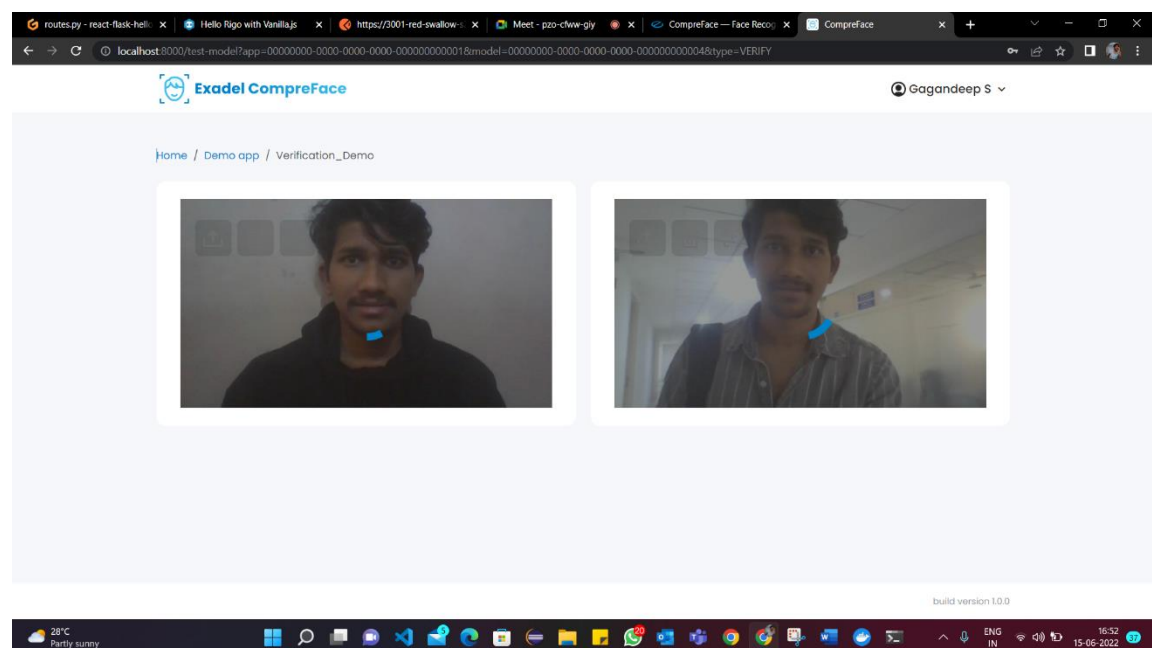


Fig 7.12: Running state for image verification.

The above Fig 7.12 ,shows the training and testing of the model.

CHAPTER 8

RESULTS(SNAPSHOTS)

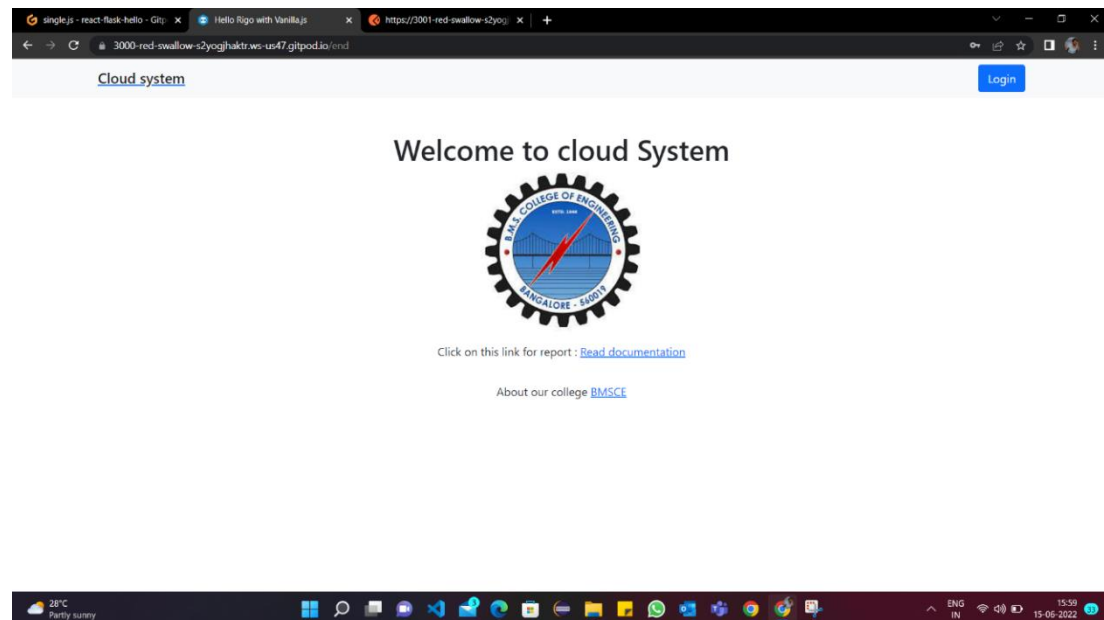


Fig 8.1: The home page

Above Fig 8.1 , shows the home page of the cloud authentication system.

It consists of two links where one will show the documentation of this project and other one is about the BMS college. After clicking the login button , login page will show up as shown in below fig 8.2.

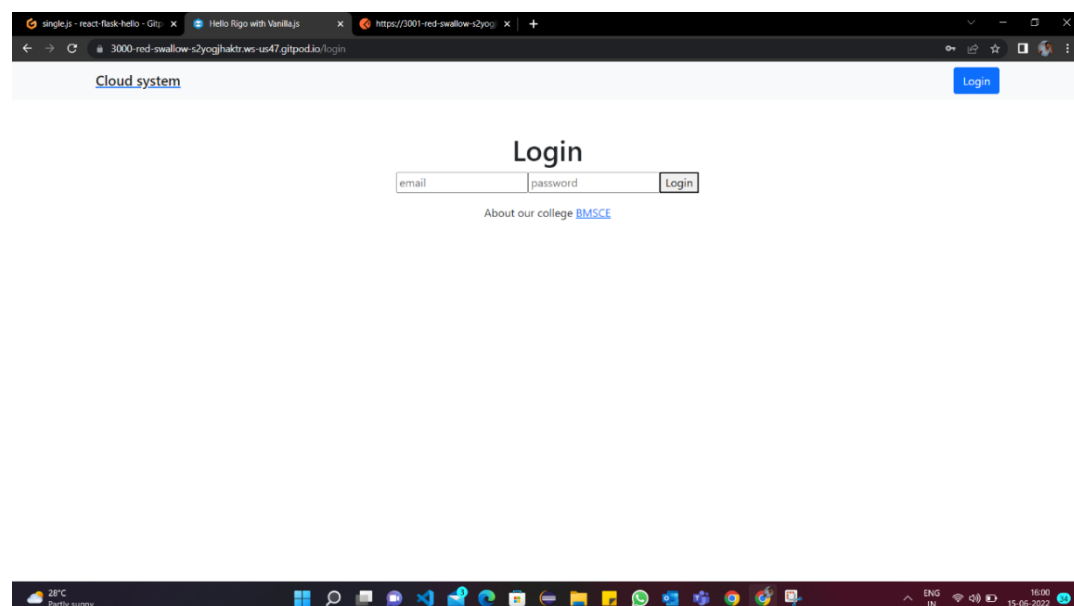


Fig 8.2: Login page

This below fig 8.3 , shows the user page after putting correct credentials in login page. It shows the name of the user entering session .

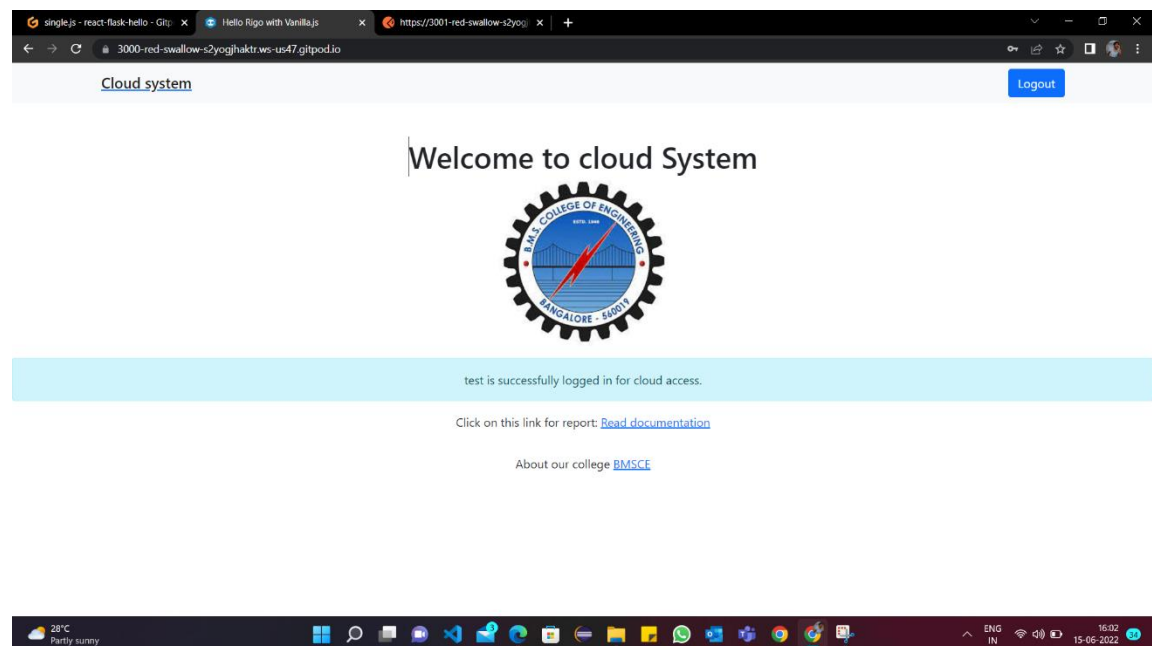


Fig 8.3: User account interface

We can see the token which was generated in postman is fetched and works as token for user session .

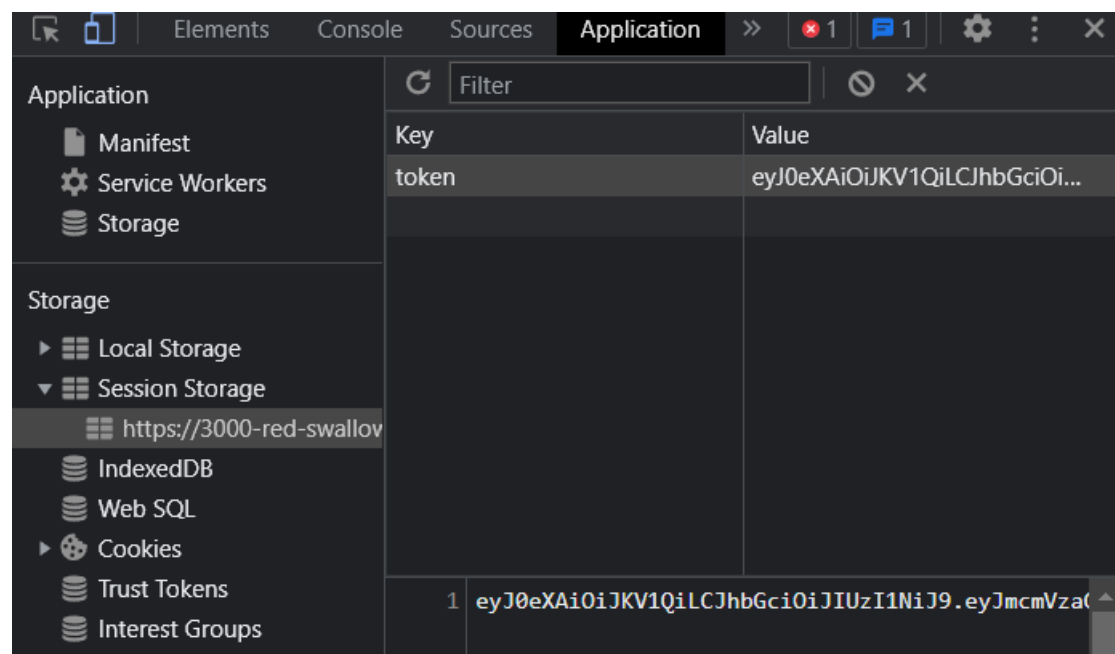


Fig 8.4: The application inspection of user session.

This also shows status , time, size of the token .

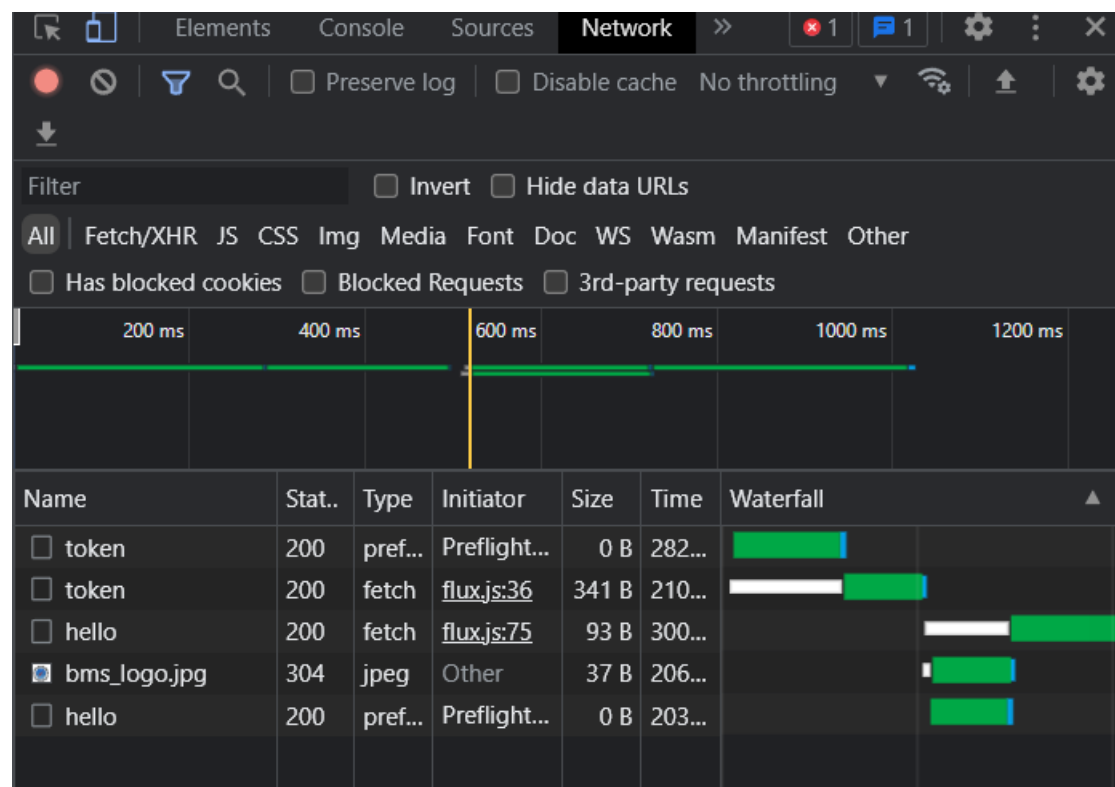


Fig 8.5: the network inspection of the user session.

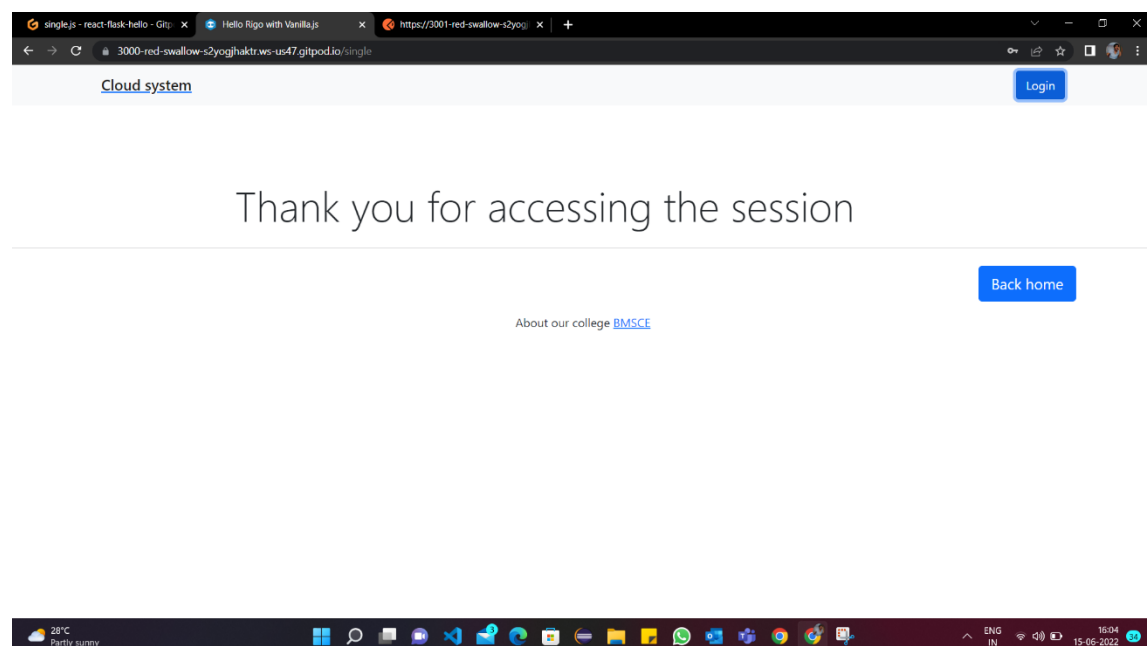


Fig 8.6: The page after the session is logged out .

After logging out , the token won't be there .It will disappear as soon as the session ends.

The below Fig 8.6 shows the verification of two images of same person where the similarity is shown as 1 , gender and age of the person .

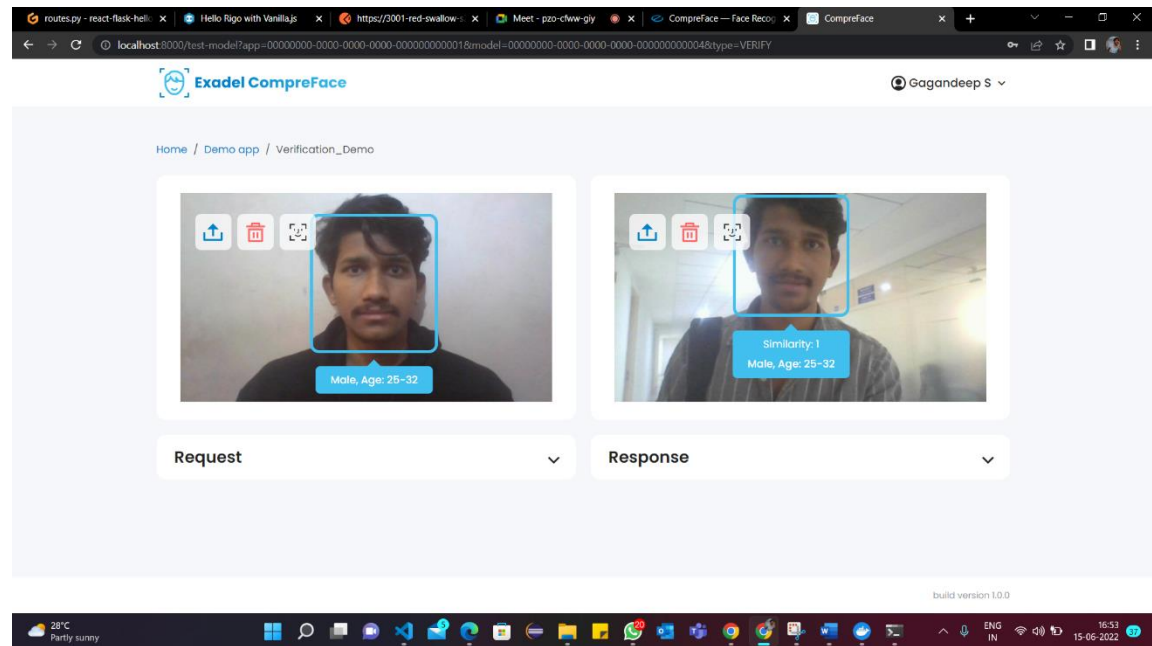


Fig 8.7: The verification of the face in compreface.

CHAPTER 9

TESTING

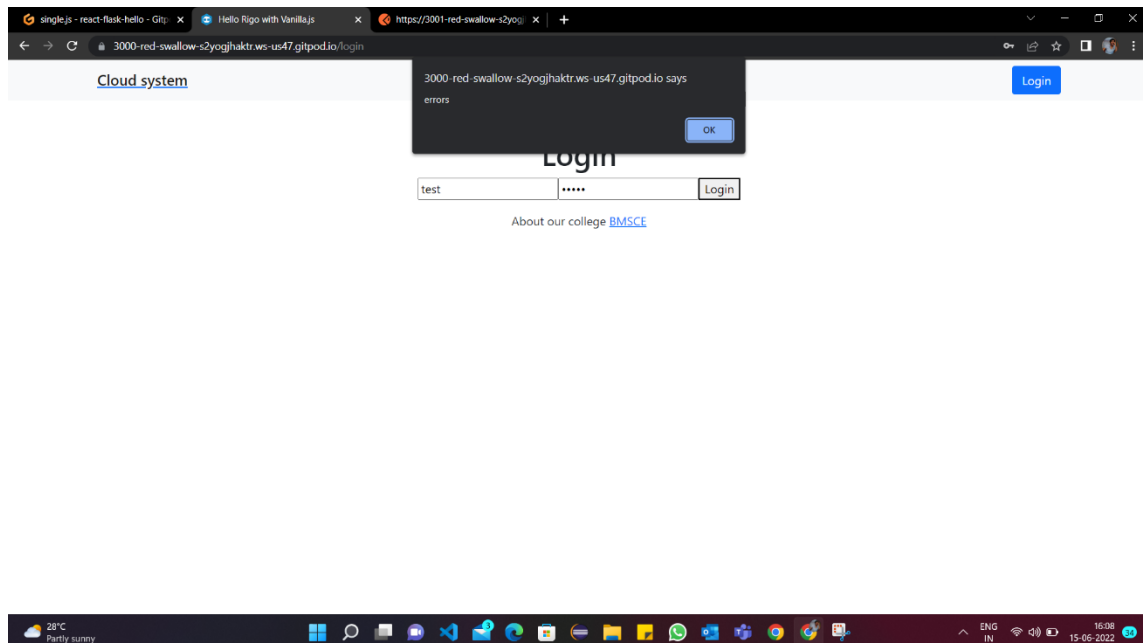


Fig 9.1 : The login in web page with wrong credentials.

The above Fig 9.1, shows the error dialog box popping up when a user gives a wrong credentials in the input form .

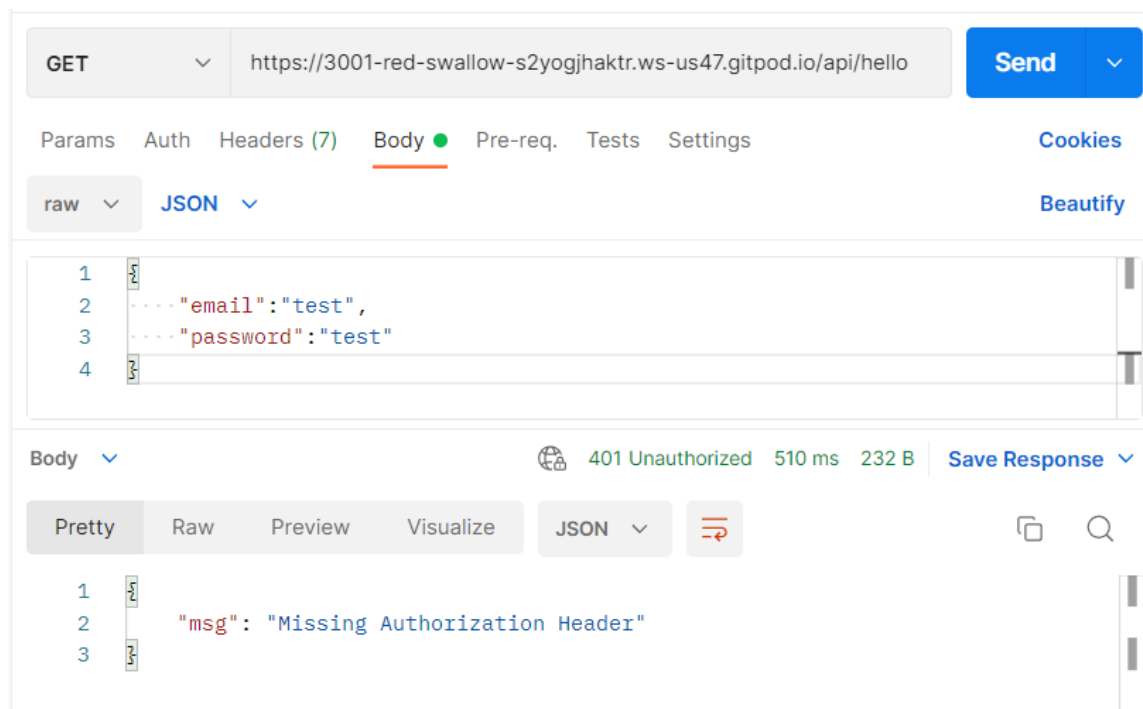


Fig 9.2 : unauthorized 401 error with missing message .

The above Fig 9.2 , shows that it will show this message when there is no header or token in matching with the header in postman.

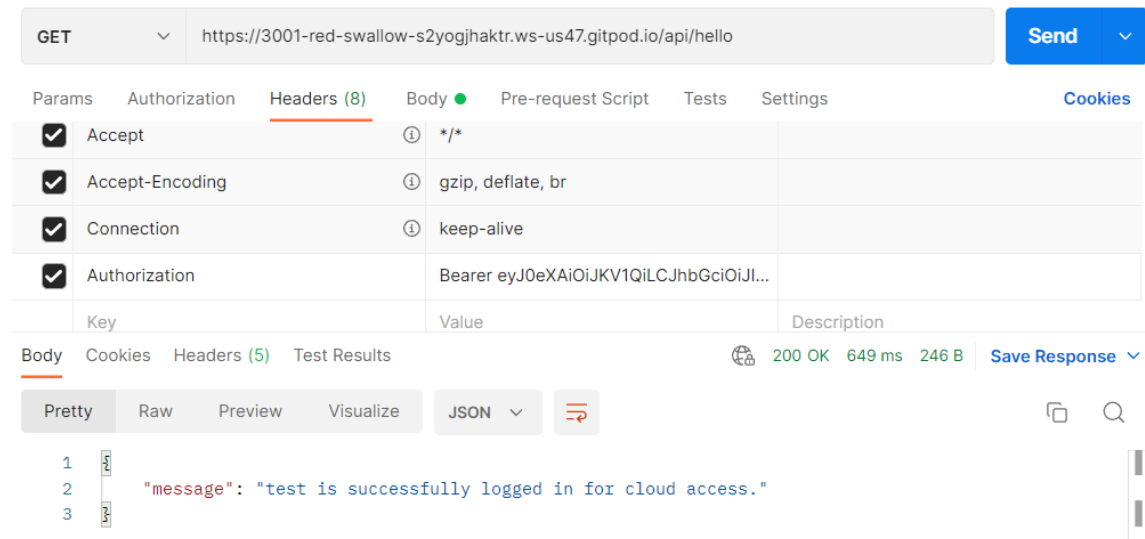


Fig 9.3 : authorized status 200 with successful message.

When we put token which was produced in the headers naming authorization it will match the header and successfully shows the message. By this way we can check the code in postman itself .

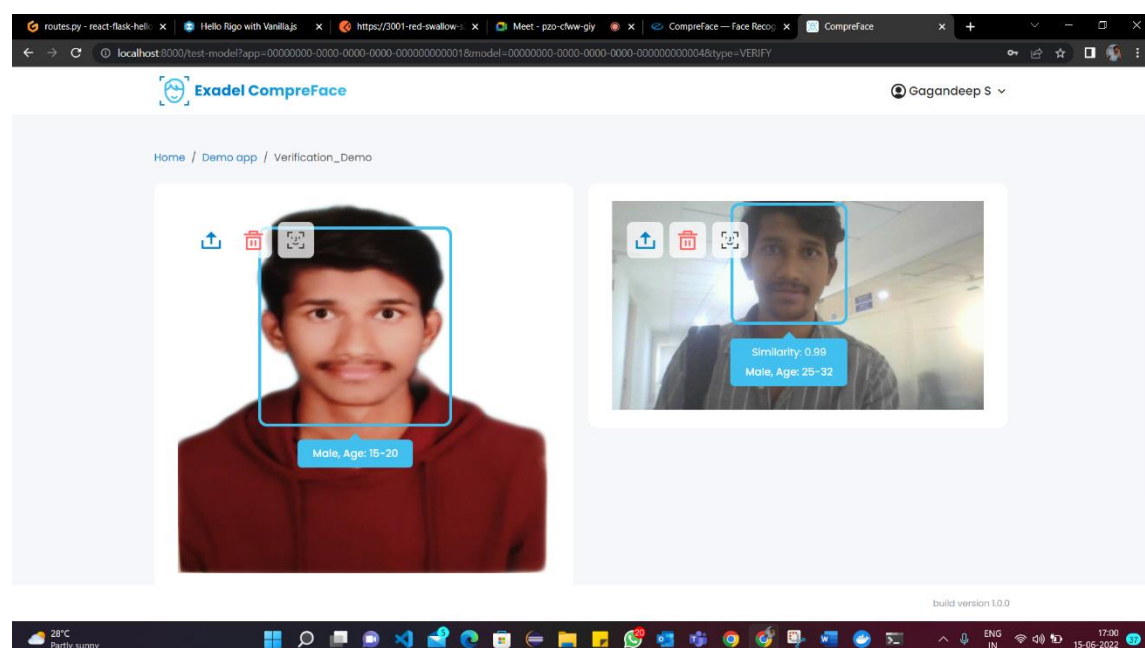


Fig 9.4: The verification of the images of same person of different age.

In Fig 9.4 ,the similarity is 0.99~1 .Hence age also a factor that determines the similarity.

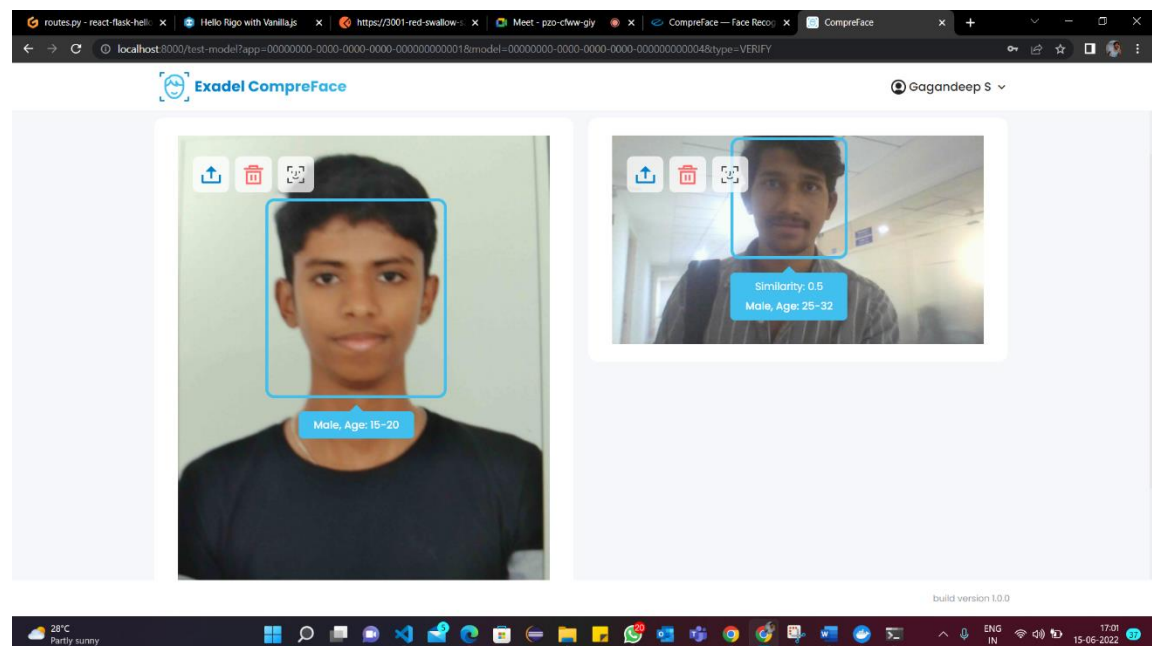


Fig 9.5: The verification of the images of different person.

Here, the similarity is 0.5 which shows that both are two different persons.

APPLICATIONS

- Provides extra security for cloud user.
- Prevention of 3rd party intervention.
- No worries of usage of data by the hosts.
- Prohibition of data deletion.
- No hampering of the data by the attacker.
- Complete trust over the system as even they can't access the data due to the security provided the cloud hosts.

CONCLUSION AND FUTURE ENHANCEMENT

With the implementation of this system, public cloud seems more secure and reliable. Since we are using external server and storage not only it's safe from third party intervention, but also it blocks the hosts from data accessing. This would solve the major concern like data hindrance, theft and many other tech related problems.

Also, we have verified an accurately working Face API, which would also be helpful for authentication.

In the near future, we will have implemented a fully operated sign up for multiple users in our authenticator and combine the FACE API in order to increase the security and make the public cloud more secure for the individuals. This allows authorized users across networks and continents to securely access information stored in the cloud with authentication provided through cloud-based services

BIBLIOGRAPHY

- [1]. Xiaodong Yang, Ping Yang, Faying An, Qixu Zhou, Miaomiao Yang ,Traceable Multi-Authority Attribute-based Encryption Scheme for cloud computing , China ,IEEE ,2017.
- [2]. Bappaditya Jana, Jayanta Poray , A Multilevel Encryption Technique in Cloud Security, West Bengal, IEEE, 2017.
- [3]. Naseer Amara, Huang Zhiqui , Awais Ali , Lahore, Cloud Computing Security Threats and Attacks with their Mitigation Techniques,China,IEEE,2017.
- [4]. Amal Ghorbel ,Mahmoud Ghorbel ,Mohamed Jmaiel ,Privacy in cloud computing environments: a survey and research challenges , New York, Springer,2017.
- [5]. Wg Cdr Nimit Kaura, Lt Col Abhishek Lal , Survey Paper on cloud computing security, India, IEEE,2017.
- [6]. Ayman M. El-Zoghby , Marianne A. Azer ,Cloud computing Privacy Issues, Challenges and Solutions,Egypt,IEEE,2017.
- [7]. Shehzad Ashraf Chaudhry¹ , Luk Kim , Seungmin Rho ,Mohammad Sabzinejad Farash , Taeshik Shon, An improved anonymous authentication scheme for distributed mobile cloud computing services,Springer,2017.
- [8]. A.Praveena , Dr.S.Smys , Ensuring Data Security in Cloud Based Social Networks, India , IEEE, 2017.
- [9]. Mr. Amit Gyandev Prajapati , Mr. Shankarlal Jayantilal Sharma , Mr. Vishal Sahebrao Badgajar ,All About Cloud : A Systematic Survey,India,IEEE,2018.

- [10]. ~~Alejandro Sanchez-Gomez, Jesus Diaz, Luis Hernandez-Encinas, and David Arroyo~~,Review of the Main Security Threats and Challenges in Free-Access Public Cloud Storage Servers,Springler,2018.
- [11]. Hussam Hourani , Mohammad Abdallah ,Cloud Computing: Legal and Security Issues,IEEE,2018.
- [12]. Srijita Basu , Arjun Bardhan, Koyal Gupta,Payel Saha, Mahasweta Pal,Manjima Bose, Kaushik Basu,Saunak Chaudhury, Pritika Sarkar ,Cloud Computing Security Challenges & Solutions-A Survey,India,IEEE,2018.
- [13]. Suryadipta Majumdar , Taous Madi, Yosr Jarraya, Makan Pourzandi, Lingyu Wang, and Mourad Debbabi Cloud Security Auditing: Major Approaches and Existing Challenges ,Canada, Springer,2019.
- [14]. N. Thillaiarasu, S. Chenthur Pandian, G. Naveen Balaji , R. M. Benitha Shierly , A. Divya , and G. Divya Prabha, Enforcing Confidentiality and Authentication over Public Cloud Using Hybrid Cryptosystems , India, Springer,2019.
- [15]. S.Pavithra , S.Ramya , Soma Prathibha ,A Survey on cloud security issues and block chain , India , IEEE, 2019.
- [16]. Srijita Basu , Arjun Bardhan, Koyal Gupta,Payel Saha, Mahasweta Pal,Manjima Bose, Kaushik Basu,Saunak Chaudhury, Pritika Sarkar ,Cloud Computing Security Challenges and its Potential Solution, India, IEEE,2019.
- [17]. Kennedy A. Torkura , Muhammad I. H. Sukmana , Feng Cheng, and Christoph Meinel ,Cloud Strike: Chaos Engineering for Security and Resiliency in Cloud Infrastructure , Germany, IEEE,2020.
- [18]. Chandler Cain , David Raymond, J. Scot Ransbottom ,The State of the Public Cloud: Security Concerns with Cloud Computing,IEEE,2020.

- [19]. Abdulmajeed Raji , Murtada Adam, Enhancing Public Cloud Security by Developing a Model For User Authentication and Data Integrity Checking, Africa, Researchgate,2020.
- [20]. Leila Megouache, Abdelhafid Zitouni and Mahieddine Djoudi, Ensuring user authentication and data integrity in multi-cloud environment, Springer, 2020.

APPENDIX A: LIST OF FIGURES

| | | |
|--------|-----------------------------------------------------|----|
| I. | System architecture diagram. | 37 |
| II. | Use case diagram.. | 38 |
| III. | Data flow diagram. | 39 |
| IV. | Installation of Flask_jwt_extended. | 41 |
| V. | Starting the server. | 42 |
| VI. | API host server. | 42 |
| VII. | Using that URL and POST method.. | 42 |
| VIII. | Putting JSON code in body | 43 |
| IX. | Access token generation.. | 43 |
| X. | login and logout actions. | 44 |
| XI. | Fetching token from the postmanLevel | 45 |
| XII. | Starting webpage | 45 |
| XIII. | code snippet of CompreFace. | 46 |
| XIV. | login in and sign in page for compreface. | 47 |
| XV. | Running state for image verification. | 47 |
| XVI. | The home page | 48 |
| XVII. | Login page | 48 |
| XVIII. | User account interface | 49 |
| XIX. | The application inspection of user session. | 49 |
| XX. | the network inspection of the user session | 50 |
| XXI. | The page after the session is logged out | 50 |
| XXII. | The verification of the face in compreface | 51 |
| XXIII. | The login in web page with wrong credentials. | 52 |
| XXIV. | unauthorized 401 error with missing message. | 53 |
| XXV. | authorized status 200 with successful message. | 53 |

| | | |
|--------|----------------------------------------------------------------------|----|
| XXVI. | The verification of the images of same person of different age. | 53 |
| XXVII. | The verification of the images of different person. | 54 |

APPENDIX B: LIST OF TABLES

| | | |
|------|---------------------------------------------|----|
| I. | Literature survey summary table 1 | 32 |
| II. | Literature survey summary table 2 | 32 |
| III. | Literature survey summary table 3 | 33 |
| IV. | Literature survey summary table 4 | 33 |
| V. | Literature survey summary table 5 | 34 |
| VI. | Literature survey summary table 6 | 34 |
| VII. | Literature survey summary table 7 | 34 |