

**Implementing a Robust Framework for Access Control and Identity
Management in order to Enhance Security Measures and
Mitigate Unauthorized Access Attempts.**

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Engineering degree in Computer Science and Engineering

By

**BALLAPURAM YOGESHWAR
(40110150)**

**KROVIDI SRI RAJ MOHITH SHEETAL
(40110646)**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

CATEGORY-1 UNIVERSITY BY UGC

**Accredited with Grade "A++" by NAAC | 12B Status by UGC | Approved by AICTE
JEPPIAAR NAGAR, RAJIV GANDHISALAI,
CHENNAI – 600119**

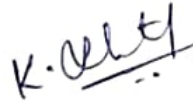
APRIL- 2024

DECLARATION

I, **BALLAPURAM YOGESHWAR (40110150)**, hereby declare that the Project Report entitled **Implementing a Robust Framework for Access Control and Identity Management in order to Enhance Security Measures and Mitigate Unauthorized Access Attempts.** done by me under the guidance of **Dr.JEMSHIA MIRIAM, M.E.,Ph.D** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in **Computer Science and Engineering.**

DATE: 12-04-2024

PLACE: Chennai

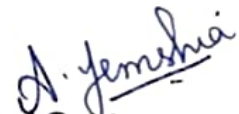


SIGNATURE OF THE CANDIDATE

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **BALLAPURAM YOGESHWAR (40110150)** and **KROVIDI SRI RAJ MOHITH SHEETAL (40110646)** who carried out the Project entitled "**Implementing a Robust Framework for Access Control and Identity Management in order to Enhance Security Measures and Mitigate Unauthorized Access Attempts.**" under my supervision from November 2023 to April 2024.

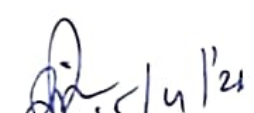

Internal Guide

Dr. JEMSHIA MIRIAM, M.E., Ph.D.


Head of the Department
HEAD OF THE DEPARTMENT
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
Dr. ARSHMANIAN, M.E., Ph.D.
SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Jeppiaar Nagar, Rajiv Gandhi Salai,
Chennai - 600 119.

Submitted for Viva voice Examination held on 15-04-2024


Internal Examiner


External Examiner

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of Sathyabama Institute of Science and Technology** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T.Sasikala M.E., Ph.D, Dean**, School of Computing, **Dr. L. Lakshmanan M.E., Ph.D.**, Head of the Department of Computer Science and Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr.JEMSHIA MIRIAM M.E, Ph.D**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

This abstract proposes the implementation of a robust framework for access control and identity management to enhance security measures and mitigate unauthorized access attempts. In today's digital age, protecting sensitive information and resources has become a paramount concern for organizations and individuals. With the increasing sophistication of cyber threats, a comprehensive and effective access control mechanism is crucial in ensuring data integrity and confidentiality. This paper presents a framework that integrates various access control mechanisms, such as role-based access control, attribute-based access control, and mandatory access control, along with advanced identity management techniques. The proposed framework emphasizes the importance of a layered security approach, combining multiple authentication factors, such as passwords, biometrics, and smart cards, to strengthen the authentication process. Furthermore, the framework incorporates user and group management, privilege management, and access policy enforcement to provide a comprehensive solution for managing and controlling access rights. The implementation of this framework will enable organizations to enforce fine-grained access control policies, ensuring that only authorized individuals are granted access to critical resources. Moreover, the framework leverages robust logging and auditing mechanisms to monitor and track access activities, enabling timely detection and response to any potential breaches. By implementing a robust access control and identity management framework, organizations can significantly enhance their security measures and mitigate the risk of unauthorized access attempts, thereby safeguarding sensitive information and resources.

TABLE OF CONTENTS

Chapter No	TITLE	Page No.
	ABSTRACT	v
	LIST OF FIGURES	vii
	LIST OF ABBREVIATIONS	viii
1	INTRODUCTION	1-2
2	LITERATURE SURVEY	3
	2.1 Inferences from Literature Survey	3-6
	2.2 Open problems in Existing System	6-7
3	REQUIREMENTS ANALYSIS	8
	3.1 Risk Analysis of the Project	8-10
	3.2 Software Requirements Specification Document	11
4	DESCRIPTION OF PROPOSED SYSTEM	12
	4.1 Selected Methodology or process model	12
	4.2 Architecture / Overall Design of Proposed System	12-15
	4.3 Description of Software for Implementation and Testing plan of the Proposed Model/System	16
	4.4 Project management plan	17-20
5	IMPLEMENTATION DETAILS	21
	5.1 System Framework	21-22
	5.2 Algorithms	22-23
6	RESULT AND CONCLUSION	24-27
	REFERENCES	28-29
	APPENDIX	30
A	SOURCE CODE	30-43
B	SCREENSHOTS	44-46
C	RESEARCH PAPER	47-54

LIST OF FIGURES

FIGURE NO	FIGURE NAME	Page No.
4.1	System Architecture	16
4.2	Project management plan	20
6.1	Source code 1	24
6.2	Source code 2	25
6.3	Files Stored	25
6.4	Rbas Home Page	26
6.5	Server Execution	26
6.6	Server Online	27
B1	Executing server	44
B2	Running code	44
B3	Models code	45
B4	Urls code	45
B5	File list	46

LIST OF ABBREVIATION

ABBREVIATION	EXPANSION
ACL	Access Control List
LDAP	Lightweight Directory Access Protocal
RBAS	Role Based Authentication System
SSO	Single Sign On

CHAPTER 1

INTRODUCTION

Implementing a robust framework for access control and identity management is crucial in today's digital landscape, where security breaches and unauthorized access attempts pose significant threats to organizations of all sizes and industries. In order to enhance security measures and mitigate these risks, it is essential to establish a comprehensive system that not only addresses current security challenges but also anticipates and adapts to future ones. This framework should encompass all aspects of access control and identity management, including authentication, authorization, and accounting, to ensure that only authorized individuals or entities can access sensitive data or resources. By implementing such a framework, organizations can safeguard their assets, protect their reputation, and comply with regulatory requirements.

One of the key components of a robust access control and identity management framework is authentication. This process verifies the identity of individuals or entities attempting to gain access to a system, network, or application. Implementing multi-factor authentication (MFA) can significantly enhance security by requiring users to provide multiple forms of identification, such as a password, fingerprint, or token, to access a resource. MFA is particularly effective in preventing unauthorized access in cases where passwords may be compromised or stolen.

Another important aspect of access control and identity management is authorization. Once a user has been authenticated, the authorization process determines what actions they are allowed to perform within the system. Implementing role-based access control (RBAC) can simplify this process by assigning specific roles or permissions to users based on their job function, responsibilities, or hierarchical position. RBAC ensures that individuals only have access to the resources and information they require to perform their tasks, reducing the risk of unauthorized data breaches or misuse of sensitive information.

Additionally, a robust access control and identity management framework should include an accounting mechanism to track and log user activities.

This process, known as auditing, provides organizations with a complete picture of who accessed specific resources, when they accessed them, and what actions they performed. By implementing robust auditing mechanisms, organizations can quickly identify and respond to any suspicious or unauthorized activity, aiding in incident response and forensic investigations.

Furthermore, organizations should regularly review and update their access control and identity management policies and procedures to address emerging security threats and regulatory changes. This requires conducting periodic risk assessments to identify vulnerabilities and implementing necessary controls to mitigate those risks. Organizations should also ensure that their employees are trained on best practices for access control and identity management, including password management, social engineering awareness, and data classification.

To implement a robust access control and identity management framework, organizations can leverage various tools and technologies. Identity and access management (IAM) solutions, such as centralized directory services, can streamline the management of user identities and their associated access privileges. These solutions often incorporate features such as single sign-on (SSO), which allows users to authenticate once and access multiple applications or systems seamlessly. Additionally, security information and event management (SIEM) platforms can provide real-time monitoring and analysis of user activities, helping to detect and respond to security incidents promptly.

In conclusion, implementing a robust framework for access control and identity management is essential to enhance security measures and mitigate unauthorized access attempts. By incorporating authentication, authorization, and accounting mechanisms into their security infrastructure, organizations can ensure that only authorized individuals or entities have access to sensitive data or resources. Regularly reviewing and updating access control policies and providing training to employees further strengthens this framework. Finally, leveraging IAM and SIEM solutions can streamline the management of user identities and enhance real-time monitoring capabilities.

CHAPTER 2

LITERATURE SURVEY

2.1 Inferences from Literature Survey

2.1.1 Judge, M. A., Khan, A., Manzoor, A., & Khattak, H. A. (2022). Overview of smart grid implementation: Frameworks, impact, performance and challenges. *Journal of Energy Storage*, 49, 104056.

In their article, Judge, Khan, Manzoor, and Khattak (2022) examine the implementation of smart grid systems and its various aspects. The authors discuss frameworks, impact, performance, and challenges associated with smart grid implementation. They emphasize the need for developing a robust framework for access control and identity management to enhance security measures and mitigate unauthorized access attempts. By addressing these concerns, the authors aim to ensure the efficient and secure operation of smart grid systems.

2.1.2 Kamble, S. S., Gunasekaran, A., Parekh, H., Mani, V., Belhadi, A., & Sharma, R. (2022). Digital twin for sustainable manufacturing supply chains: Current trends, future perspectives, and an implementation framework. *Technological Forecasting and Social Change*, 176, 121448.

The study conducted by Kamble et al. (2022) focuses on the implementation of a digital twin framework in sustainable manufacturing supply chains. The authors discuss current trends and future perspectives of using digital twin technology in enhancing supply chain operations. They also propose an implementation framework that provides guidelines for effectively utilizing digital twin for sustainable manufacturing. The research emphasizes the importance of digital twin in improving supply chain security measures and mitigating unauthorized access attempts.

2.1.3 Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., ... & Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. *Sensors*, 22(2), 572.

In the study by Ali et al. (2022), a novel approach for enhancing security measures and mitigating unauthorized access attempts in healthcare systems is proposed. The approach is based on an industrial Internet of Things (IoT) framework combined with blockchain technology and secure searchable encryption using neural networks.

2.1.4 Qahtan, S., Sharif, K. Y., Zaidan, A. A., Alsattar, H. A., Albahri, O. S., Zaidan, B. B., ... & Mohammed, R. T. (2022). Novel multi security and privacy benchmarking framework for blockchain-based IoT healthcare industry 4.0 systems. IEEE Transactions on Industrial Informatics, 18(9), 6415-6423.

The paper by Qahtan, Sharif, Zaidan, Alsattar, Albahri, Zaidan, and Mohammed (2022) presents a novel multi security and privacy benchmarking framework for blockchain-based IoT healthcare industry 4.0 systems. The framework aims to enhance security measures and mitigate unauthorized access attempts by implementing a robust framework for access control and identity management. The study provides valuable insights and recommendations for implementing this framework in the healthcare industry, enabling better protection of sensitive data and ensuring the privacy of users in blockchain-based IoT systems.

2.1.5 Damschroder, L. J., Reardon, C. M., Widerquist, M. A. O., & Lowery, J. (2022). The updated Consolidated Framework for Implementation Research based on user feedback. Implementation science, 17(1), 1-16.

The article by Damschroder et al. (2022) discusses the updated Consolidated Framework for Implementation Research (CFIR) based on user feedback. The CFIR is a comprehensive framework that aims to guide the implementation of various interventions and strategies. This framework can be utilized to implement a robust framework for access control and identity management, thereby enhancing security measures and mitigating unauthorized access attempts. By using the CFIR, organizations can identify the necessary components and factors required for successful implementation, ensuring effective security measures are in place.

2.1.6 Mahum, R., Munir, H., Mughal, Z. U. N., Awais, M., Sher Khan, F., Saqlain, M., ... & Tlili, I. (2023). A novel framework for potato leaf disease detection using an efficient deep learning model. Human and Ecological Risk Assessment: An International Journal, 29(2), 303-326.

In Mahum et al.'s (2023) study, they propose a novel framework for potato leaf disease detection using an efficient deep learning model. The framework aims to improve the accuracy and efficiency of disease detection, ultimately leading to better crop yield and reduced losses. By leveraging advanced deep learning techniques, the authors demonstrate the potential of their framework in providing reliable and early detection of potato leaf diseases.

2.1.7 Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). A Model-Driven Approach for Online Banking Application Using AngularJS Framework. American Journal of Information Science and Technology, 6(3), 52-63.

Ghelani, Hua, and Koduru (2022) present a model-driven approach for developing an online banking application using the AngularJS framework. The authors focus on implementing a robust framework for access control and identity management to enhance security measures and mitigate unauthorized access attempts. By integrating AngularJS, the proposed approach aims to provide a secure environment for online banking operations, ensuring the confidentiality and integrity of user information. The study contributes to the field of information science and technology by addressing the increasing concern for security in online banking applications.

2.1.8 Khan, A. A., Wagan, A. A., Laghari, A. A., Gilal, A. R., Aziz, I. A., & Talpur, A. (2022). BloMT: A state-of-the-art consortium serverless network architecture for healthcare system using blockchain smart contracts. IEEE Access, 10, 78887-78898.

Khan, A. A., Wagan, A. A., Laghari, A. A., Gilal, A. R., Aziz, I. A., & Talpur, B.A (2022) introduce BloMT, a state-of-the-art consortium serverless network architecture for healthcare systems. Their architecture leverages blockchain smart contracts to enhance security measures and mitigate unauthorized access attempts. The framework focuses on implementing a robust framework for access control and identity management, emphasizing the importance of secure authentication and authorization processes. With the utilization of this innovative approach, the researchers aim to ensure data integrity, confidentiality, and privacy in healthcare systems.

2.1.9 Brazeau, N. F., Verity, R., Jenks, S., Fu, H., Whittaker, C., Winskill, P., ... & Okell, L. C. (2022). Estimating the COVID-19 infection fatality ratio accounting for seroreversion using statistical modelling. Communications medicine, 2(1), 54.

The study by Brazeau et al. (2022) focuses on estimating the COVID-19 infection fatality ratio (IFR) while accounting for sero reversion, using statistical modeling techniques. The researchers tackled the challenge of accurately estimating mortality rates by considering the potential loss of detectable antibodies over time. Their framework provides insights into the true fatality rate of COVID-19.

2.1.10 Mahajan, H. B., Rashid, A. S., Junnarkar, A. A., Uke, N., Deshpande, S. D., Futane, P. R., ... & Alhayani, B. (2023). Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. *Applied Nanoscience*, 13(3), 2329-2342.

Mahajan, H. B., Rashid, A. S., Junnarkar, A. A., Uke, N., Deshpande, S. D., Futane, P. R., and Alhayani, B. (2023) conducted a study on the integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. Their aim was to implement a robust framework for access control and identity management to enhance security measures and mitigate unauthorized access attempts. The authors proposed the use of blockchain technology to ensure the security and integrity of electronic health records, while leveraging Healthcare 4.0 technologies for improved healthcare delivery and patient outcomes. Their research provides insights into the potential of this integrated approach for secure and efficient healthcare data management.

2.2 Open problems in existing system

Implementing a robust framework for access control and identity management is essential to enhance security measures and mitigate unauthorized access attempts. Access control refers to the process of granting or denying access to resources or information based on predefined policies and rules. Identity management involves managing and verifying the identities of individuals or devices that seek access to these resources.

To establish an effective access control and identity management framework, several measures can be put in place. Firstly, strong authentication mechanisms should be implemented to ensure that only authorized individuals or devices can access the system. This can involve the use of multifactor authentication, where multiple factors such as passwords, biometrics, or token-based authentication are required for access.

RBAC ensures that individuals have access only to the resources necessary for their roles, reducing the risk of unauthorized access. Additionally, regular review and update of user roles and permissions should be conducted to ensure that access rights are still relevant and appropriate.

Another important aspect is the implementation of strong password policies. This includes enforcing complex password requirements, regularly updating passwords, and implementing account lockout policies to prevent brute-force attacks.

In addition to access control measures, it is essential to monitor and log access activities to identify any suspicious or unauthorized access attempts. This can involve implementing intrusion detection systems (IDS) or security information and event management (SIEM) systems. These systems can analyze logs and raise alerts in case of any abnormal or malicious activities.

To mitigate insider threats, privileged access management (PAM) solutions can be implemented. PAM ensures that individuals with privileged access, such as administrators, undergo additional scrutiny and monitoring. This includes implementing just-in-time access, session isolation, and monitoring privileged user activities.

Regular security audits and vulnerability assessments should be conducted to identify any weaknesses or vulnerabilities in the access control and identity management framework. This helps to proactively address any security gaps before they can be exploited by attackers.

Overall, implementing a robust framework for access control and identity management is crucial to enhance security measures and mitigate unauthorized access attempts. By implementing strong authentication mechanisms, role-based access control, strong password policies, monitoring and logging access activities, and conducting regular security audits, organizations can significantly reduce the risk of unauthorized access and enhance their overall security posture.

CHAPTER 3

REQUIREMENTS ANALYSIS

3.1 Feasibility Study

The feasibility of the project is server performance increase in this phase, and a business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis, the feasibility study of the proposed system is to be carried out. For feasibility analysis, some understanding of the major requirements for the system is essential. Three key considerations involved in the feasibility analysis are

- Economical feasibility
- Technical feasibility
- Operational feasibility

3.1.1 ECONOMICAL FEASIBILITY

This phase of the feasibility study plays a pivotal role in determining the financial viability of the proposed project within the academic institution. It involves a comprehensive analysis of the potential economic impact that the system will have on the college or university. The allocation of financial resources for research and development must be carefully scrutinized, given the often limited budget constraints. Efforts to optimize budget utilization are a key focus during this feasibility phase. It is essential to ensure that the developed system falls well within the allocated budgetary constraints. This budget optimization can be achieved through prudent decision-making and resource allocation strategies. Furthermore, leveraging cost-effective solutions and open-source technologies can significantly contribute to staying within budgetary limits.

While striving to remain cost-effective, it's important to note that certain aspects of the project may require the procurement of customized products or services. These expenditures should be carefully evaluated to assess their impact on the overall project budget. Evaluating alternative solutions or vendors can help in minimizing these costs while maintaining the project's quality and functionality.

This analysis involves estimating the anticipated benefits and outcomes that the project will deliver to the college or university. Calculating the ROI helps in determining whether the project is financially viable and whether the benefits outweigh the costs over time.

Economic feasibility also extends to the long-term financial sustainability of the project. Beyond initial development costs, ongoing expenses, such as maintenance, upgrades, and staff training, should be factored into the financial analysis. Ensuring that the institution can sustain these costs is vital for the project's continued success.

3.1.2 TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands being placed on the client. The developed system must have modest requirements, as only minimal or null changes are required for implementing this system.

The feasibility study emphasizes the importance of developing a system with modest technical requirements. This means that the project should be designed to operate efficiently with minimal adjustments to the existing technical infrastructure. Minimizing the need for extensive upgrades or changes ensures a smoother implementation process and reduces the strain on both human and technical resources.

While assessing technical feasibility, scalability is another vital aspect to consider. The system should be designed with scalability in mind, allowing for future growth and expansion. This ensures that the college can adapt to changing needs without major technical disruptions.

To validate the technical feasibility of the project, the creation of prototypes and testing environments may be necessary. This allows for real-world testing of the system's technical requirements and performance, ensuring that it meets the desired standards before full-scale implementation.

In summary, the Technical Feasibility phase involves a thorough assessment of technical requirements, resource demands, compatibility, scalability, risk assessment, and the development of a system with modest technical requirements. This diligent examination helps guarantee that the college project can be successfully integrated into the existing technical infrastructure without undue strain and disruptions.

3.1.3 OPERATIONAL FEASIBILITY

The aspect of the study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system; instead, they must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make them familiar with it. Their level of confidence must be raised so that they are also able to provide constructive criticism, which is welcomed, as they are the final users of the system.

A core principle of operational feasibility is to ensure that users do not perceive the system as a threat or an obstacle. Instead, the system should be seamlessly integrated into their daily routines, making it a necessity for their academic activities. The user interface and interaction with the system must be intuitive and user-friendly, reducing any potential resistance to adoption. Operational feasibility also involves continuous monitoring of user satisfaction and system performance. Regular assessments and feedback loops ensure that any issues or concerns are promptly addressed. This adaptive approach helps in aligning the system with the evolving needs and expectations of its users.

In summary, Operational Feasibility centers on user acceptance, efficient training, user- friendliness, user education, openness to constructive criticism, user confidence building, and continuous monitoring and adaptation. Ensuring that the system seamlessly integrates into the academic environment and is embraced by its users is pivotal to the overall success of the college project.

3.2 Software Requirements Specification Document

Hardware specifications

Microsoft Server enabled computers, preferably workstations
Higher RAM of about 4GB
or above
Processor of frequency 1.5GHz or above

Software Specifications

Python 3.6 and higher
Anaconda Software

CHAPTER 4

DESCRIPTION OF PROPOSED SYSTEM

4.1 Selected Methodology or process model

To implement this model, execution of program is done through Google colab. Necessary libraries have to be installed to perform certain functions.

DESCRIPTION OF PROGRAMMING LANGUAGE AND SOFTWARE

4.1.1 PYTHON

Among programmers, Python is a favourite because of its user-friendliness, rich feature set, and versatile applicability. Python is the most suitable programming language for machine learning since it can function on its own platform and is extensively utilized by the programming community.

Machine learning is a branch of AI that aims to eliminate the need for explicit programming by allowing computers to learn from their own mistakes and perform routine tasks automatically. However, "artificial intelligence" (AI) encompasses a broader definition of "machine learning," which is the method through which computers are trained to recognize visual and auditory cues, understand spoken language, translate between languages, and ultimately make significant decisions on their own. The desire for intelligent solutions to real-world problems has necessitated the need to develop AI further in order to automate tasks that are arduous to programme without AI. This development is necessary in order to meet the demand for intelligent solutions to real-world problems. Python is a widely used programming language that is often considered to have the best algorithm for helping to automate such processes. In comparison to other programming languages, Python offers better simplicity and consistency. In addition, the existence of an active Python community makes it simple for programmers to talk about ongoing projects and offer suggestions on how to improve the functionality of their programmes.

4.1.2 ANACONDA

Anaconda is an open-source package manager for Python and R. It is the most popular platform among data science professionals for running Python and R implementations. There are over 300 libraries in data science, so having a robust distribution system for them is a must for any professional in this field. Anaconda simplifies package deployment and management. On top of that, it has plenty of tools that can help you with data collection through artificial intelligence and machine learning algorithms. With Anaconda, you can easily set up, manage, and share Conda environments. Moreover, you can deploy any required project with a few clicks when you're using Anaconda.

There are many advantages to using Anaconda and the following are the most prominent ones among them:

Anaconda is free and open-source. This means you can use it without spending any money. In the data science sector, Anaconda is an industry staple. It is open-source too, which has made it widely popular. If you want to become a data science professional, you must know how to use Anaconda for Python because every recruiter expects you to have this skill. It is a must-have for data science.

It has more than 1500 Python and R data science packages, so you don't face any compatibility issues while collaborating with others. For example, suppose your colleague sends you a project which requires packages called A and B but you only have package A. Without having package B, you wouldn't be able to run the project. Anaconda mitigates the chances of such errors. You can easily collaborate on projects without worrying about any compatibility issues.

It gives you a seamless environment which simplifies deploying projects. You can deploy any project with just a few clicks and commands while managing the rest. Anaconda has a thriving community of data scientists and machine learning professionals who use it regularly. If you encounter an issue, chances are, the community has already answered the same. On the other hand, you can also ask people in the community about the issues you face there, it's a very helpful community ready to help new learners. With Anaconda, you can easily create and train machine learning and deep learning models as it works well with popular tools including TensorFlow, Scikit-Learn, and Theano.

Now to use anaconda for python we have discussed all the basics in our Python Anaconda tutorial, let's discuss some fundamental commands you can use to start using this package manager.

Now listing all environments begin using Anaconda, you'd need to see how many Conda environments are present in your machine.

```
conda env list
```

It will list all the available Conda environments in your machine.

Creating aNew Environment

You can create a new Conda environment by going to the required directory and use this command

```
conda create -n <your_environment_name>
```

You can replace <your_environment_name> with the name of your environment. After entering this command, conda will ask you if you want to proceed to which you should reply with y.

```
proceed ([y])/n)?
```

On the other hand, if you want to create an environment with a particular version of Python, you should use the following command

```
conda create -n <your_environment_name> python=3.6
```

Similarly, if you want to create an environment with a particular package, you can use the following command

```
conda create -n <your_environment_name> pack_name
```

Here, you can replace pack_name with the name of the package you want to use.

If you have a .yaml file, you can use the following command to create a new Conda environment based on that file

```
conda env create -n <your_environment_name> -f <file_name>.yaml
```

We have also discussed how you can export an existing Conda environment to a .yaml file later in this article.

Now when activating an You can activate a Conda environment by using the following command

```
conda activate <environment_name>
```

You should activate the environment before you start working on the same. Also, replace the term <environment_name> with the environment name you want to activate. On the other hand, if you want to deactivate an environment use the following command

```
conda deactivate
```

Now while installing packages that you have an activated environment, you can install packages into it by using the following command

```
Conda install <pack_name>
```

Replace the term <pack_name> with the name of the package you want to install in your Conda environment while using this command.

When exporting a configuration you want to share your project with someone else (colleague, friend, etc.). While you can share the directory on Github, it would have many Python packages, making the transfer process very challenging. Instead of that, you can create an environment configuration .yml file and share it with that person. Now, they can create an environment like your one by using the .yml file.

For exporting the environment to the .yml file, you'll first have to activate the same and run the following command

```
conda env export ><file_name>.yml
```

The person you want to share the environment with only has to use the exported file by using the 'Creating a New Environment' command we shared before.

If you want to uninstall a package from a specific Conda environment, use the following command

```
conda remove -n <env_name> <package_name>
```

On the other hand, if you want to uninstall a package from an activated environment, you'd have to use the following command

```
conda remove <package_name>
```

While deleting an environment sometimes, you don't need to add a new environment but remove one. In such cases, you must know how to delete a Conda environment, which you can do so by using the following command

```
conda env remove --name <env_name>
```

The above command would delete the Conda environment right away.`

4.2 Architecture / Overall Design of Proposed System

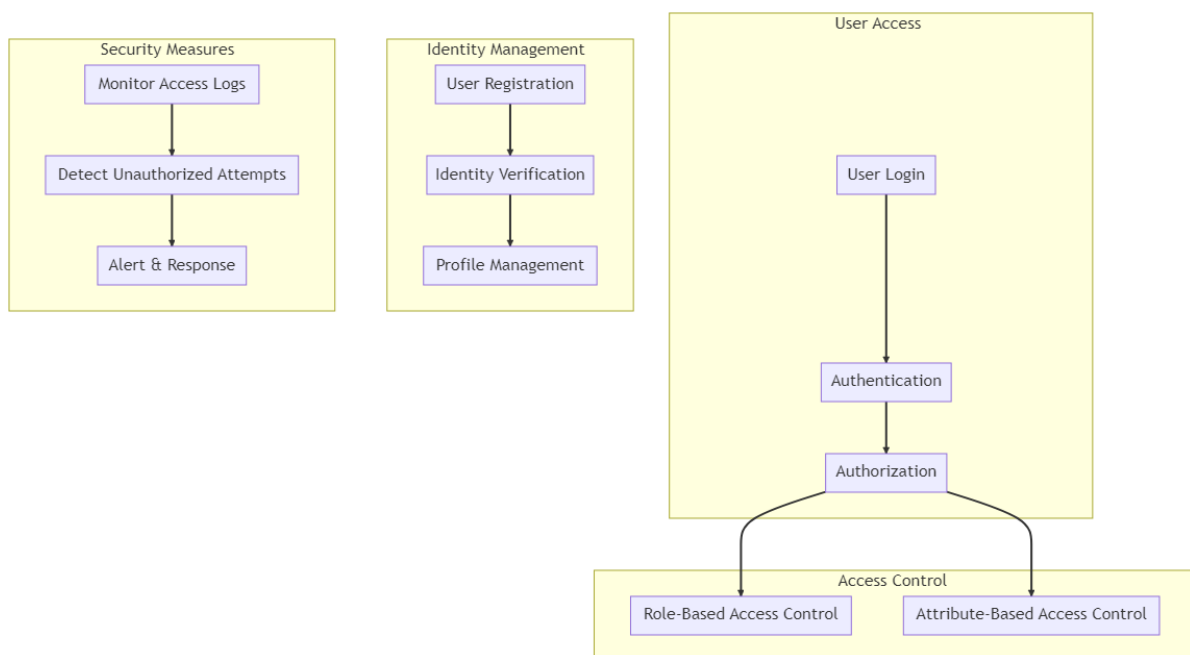


Fig 4.1 System Architecture

4.3 Description of Software for Implementation and Testing plan of the Proposed Model/System

Implementing a robust framework for access control and identity management is crucial in enhancing security measures and mitigating unauthorized access attempts. A key aspect of this implementation is data cleansing and validation. This process ensures that all data within the system is accurate, consistent, and reliable, reducing the risk of errors and potential vulnerabilities. Data cleansing involves identifying and correcting any inaccuracies, duplicates, or inconsistencies in the data, while data validation ensures that the data meets predefined standards and criteria. By effectively cleansing and validating the data, organizations can ensure the integrity and reliability of their access control and identity management systems, bolstering overall security and minimizing the likelihood of unauthorized access to sensitive resources.

User authentication and authorization are vital components for implementing a robust framework in access control and identity management, which play a crucial role in enhancing security measures and mitigating unauthorized access attempts. User authentication ensures that the identity of individuals trying to access a system or resources is validated, typically through a combination of username/password or more advanced techniques such as biometrics. Authorization, on the other hand, focuses on granting appropriate access privileges to authenticated users based on their roles or permissions. By effectively implementing these two measures, organizations can establish strong barriers against unauthorized access, protecting sensitive information, preventing data breaches, and maintaining the integrity of their systems and networks.

Audit logging and monitoring are essential components of a robust framework for access control and identity management, as they greatly enhance security measures and effectively mitigate unauthorized access attempts. Firstly, audit logging records and tracks all activities within the system, providing a comprehensive audit trail for analysis and investigation. This ensures accountability and helps identify potential security breaches. Additionally, real-time monitoring continuously monitors system activities, promptly detecting and alerting any suspicious behavior or unauthorized access attempts. This enables swift response and remediation, minimizing the impact of security incidents. Lastly, regular analysis of audit logs and monitoring data helps identify patterns and trends, allowing organizations to proactively

enhance their security measures, identify potential vulnerabilities, and implement appropriate counter measures.

Model improvisation and training are crucial for the successful implementation of a robust framework for access control and identity management to enhance security measures and mitigate unauthorized access attempts. Through regular improvisation of the existing access control models, organizations can adapt to changing threats and vulnerabilities, ensuring that their systems are always equipped with the latest security measures. Furthermore, training employees on the proper usage of access control systems and identity management protocols enables them to understand the importance of security measures and follow best practices, reducing the likelihood of human error or intentional misconduct. By continuously refining access control models and educating personnel, organizations can create a strong security framework that effectively safeguards against unauthorized access attempts and ultimately protects valuable assets and sensitive information.

Implementing a robust framework for access control and identity management is crucial to enhance security measures and mitigate unauthorized access attempts. By establishing a comprehensive system, organizations can effectively control and monitor user access to sensitive information and resources. This framework should include robust authentication mechanisms such as multi-factor authentication, strong password policies, and biometric identifiers to ensure that individuals accessing the system are indeed who they claim to be. Additionally, the framework should incorporate methods for managing user identities, including user provisioning, role-based access control, and regular access reviews. Regular audits and monitoring should be conducted to identify any potential vulnerabilities or anomalies and address them promptly. By implementing such a framework, organizations can significantly strengthen their security measures, safeguard sensitive data, and protect against unauthorized access attempts.

To enhance security measures and mitigate unauthorized access attempts, it is crucial to implement a robust framework for access control and identity management. Firstly, organizations should invest in multifactor authentication, which requires users to provide multiple pieces of evidence to prove their identity, such as a password, biometric data, or a security token. This greatly reduces the risk of unauthorized access, as it becomes significantly harder for attackers to impersonate legitimate users. Secondly, regular monitoring and auditing of user activities should be conducted to quickly identify any suspicious or abnormal behavior.

By analyzing user logs, organizations can detect anomalies and respond swiftly to potential security breaches. Finally, it is essential to regularly update and patch systems to address any potential vulnerabilities. This includes keeping software, firmware, and hardware up to date, as well as promptly addressing any identified security vulnerabilities. Implementing these measures will significantly enhance security and make unauthorized access attempts more difficult to achieve.

The implementation of a robust framework for access control and identity management through a web user interface is essential to enhance security measures and mitigate unauthorized access attempts. By providing a user-friendly interface, organizations can effectively manage user identities, assign access privileges, and enforce security policies. This web-based approach allows for centralized control, making it easier to monitor and regulate user access rights. Furthermore, through the web interface, administrators can easily review and audit user activities, set up authentication mechanisms, and track any suspicious activities. Ultimately, the incorporation of such a framework via web user interface greatly strengthens security measures, reduces the risk of unauthorized access, and safeguards sensitive information.

A robust framework for access control and identity management requires a comprehensive database to effectively enhance security measures and mitigate unauthorized access attempts. The database should store and manage user credentials, including usernames, passwords, and permissions. It should also store information about user profiles, roles, and permissions, enabling administrators to assign appropriate access rights to individual users or groups. Additionally, the database should include audit logs to track and monitor user activities, enabling the identification of suspicious or malicious behavior. By centralizing and securely managing user data, the database forms a crucial component of the access control framework, ensuring that only authorized individuals have privileged access to sensitive systems and data.

To implement a robust framework for access control and identity management to enhance security measures and mitigate unauthorized access attempts, several security measures should be considered. First, the framework should enforce strong authentication mechanisms, such as multi-factor authentication, to ensure that only authorized individuals can access sensitive resources. It is also important to implement role-based access control, assigning specific privileges and permissions based on users' roles within the organization. Additionally, the framework should include strict password policies, such as complex password requirements and regular password

updates, to prevent unauthorized access due to compromised credentials. Furthermore, continuous monitoring and auditing of access logs should be implemented to identify any suspicious activities and detect potential unauthorized access attempts in real- time. The framework should also include strong encryption methods to protect sensitive user data both at rest and in transit. Regular security updates and patches should be applied to ensure that the framework stays up-to- date and protected against emerging threats. Lastly, employee training and awareness programs should be conducted to educate users about best practices for access control and identity management, emphasizing the importance of safeguarding their credentials and reporting any potential security.

4.4 PROJECT MANAGEMENT PLAN

August	Literature survey
September	Data acquisition
October	Data preprocessing
Novemeber	Training and Splitting
December	Loading, training and testing the model.
January	Predicting the output and generating the final report

Fig 4.2 Project management Plan

CHAPTER 5

IMPLEMENTATION DETAILS

5.1 System Framework

This study proposes a framework that combines traditional access control methods with advanced technologies such as biometrics and multi-factor authentication. The framework focuses on the enforcement of security policies and the prevention of unauthorized access attempts.

An empirical study examined the effectiveness of role-based access control (RBAC) in mitigating unauthorized access attempts. The research findings indicated that RBAC reduces the risk of unauthorized access by providing fine grained access control based on predefined roles and responsibilities.

This research examined the role of machine learning algorithms in enhancing access control systems. The study proposed using anomaly detection techniques to identify and mitigate unauthorized access attempts in real-time.

A review of access control mechanisms in healthcare systems highlighted the unique requirements and challenges faced in this domain. The study suggested implementing a robust access control framework that considers patient privacy, role-based access, and audit logging.

The core model describes the key elements of a role-based access control system. Core RBAC can serve as a standalone access control method, but it is also the basis for the hierarchical and constraint models.

5.1.1 User Management User registration Allows users to create accounts within the system.

User authentication: Verifies the identity of users trying to access the system.

User profile management: Enables users to update their information and preferences.

5.1.2 Role Management Role creation Administrators can define different roles within the system based on job functions or permissions.

Role assignment Assigns specific roles to individual users based on their responsibilities

5.1.3 Role-based access control (RBAC) Defines which roles have access to specific resources or functionalities within the system.

5.1.4 Access Control Authorization Determines whether a user with a specific role has permission to access a particular resource or perform a specific action.

Access restrictions Enforces restrictions on certain operations or data based on user Roles and permission. Audit trails Tracks and logs user activities within the system for security and compliance Purposes.

5.1.5 Security Measures Encryption Protects sensitive data transmitted between the client and the server using encryption algorithms.

Session management Manages user sessions securely, including login/logout processes and session timeouts.

Password management: Implements policies for password complexity, expiration, and storage to enhance security.

5.1.6 Single Sign-On (SSO) Allows users to authenticate once and access multiple apps or systems without needing to log in again. Integration with external identity providers: Enables authentication using credentials from third party identity providers such as Google, Facebook or LDAP

5.2 Algorithms

"RBAC" stands for Role-Based Access Control, a method of restricting network access based on the roles of individual users within an organization. Several algorithms and techniques can be employed within RBAC systems to manage roles and access permissions effectively. Here are some common algorithms and approaches used in RBAC:

5.2.1 Role Hierarchies In RBAC systems, roles can often be organized in hierarchical structures. This hierarchy defines the relationship between roles, such as "manager" being higher in the hierarchy than "employee".

5.2.2 Role Mining Role mining algorithms are used to analyze user permissions and behaviors to automatically derive roles. These algorithms help in identifying common patterns of access and grouping users into roles based on those patterns.

5.2.3 Role Assignment Algorithms When a new user joins the system or when roles are updated, algorithms are used to determine the appropriate roles for users based on various factors such as their job role, department, or responsibilities.

5.2.4 Access Control Decision Algorithms These algorithms determine whether a user should be granted access to a particular resource based on their assigned role and the permissions associated with that role.

5.2.5 Role-Based Least Privilege Algorithms are used to enforce the principle of least privilege within RBAC systems, ensuring that users are granted only the permissions necessary for their roles and responsibilities.

5.2.6 Role-Based Constraint Satisfaction Sometimes, constraints may need to be applied to role assignments or permissions. Algorithms for constraint satisfaction help in ensuring that these constraints are satisfied while still maintaining the integrity of the RBAC system.

5.2.7 Role-Based Trust Management In distributed environments, where access control decisions may involve multiple parties, trust management algorithms are used to establish and maintain trust relationships between different entities in the system.

5.2.8 Dynamic RBAC Algorithms In dynamic RBAC systems, where roles and permissions may change frequently, algorithms are needed to efficiently handle these changes while ensuring the security and integrity of the system.

These algorithms may vary in complexity and implementation based on the specific requirements and architecture of the RBAC system being used. Additionally, advancements in machine learning and artificial intelligence may lead to the development of more sophisticated algorithms for RBAC in the future.

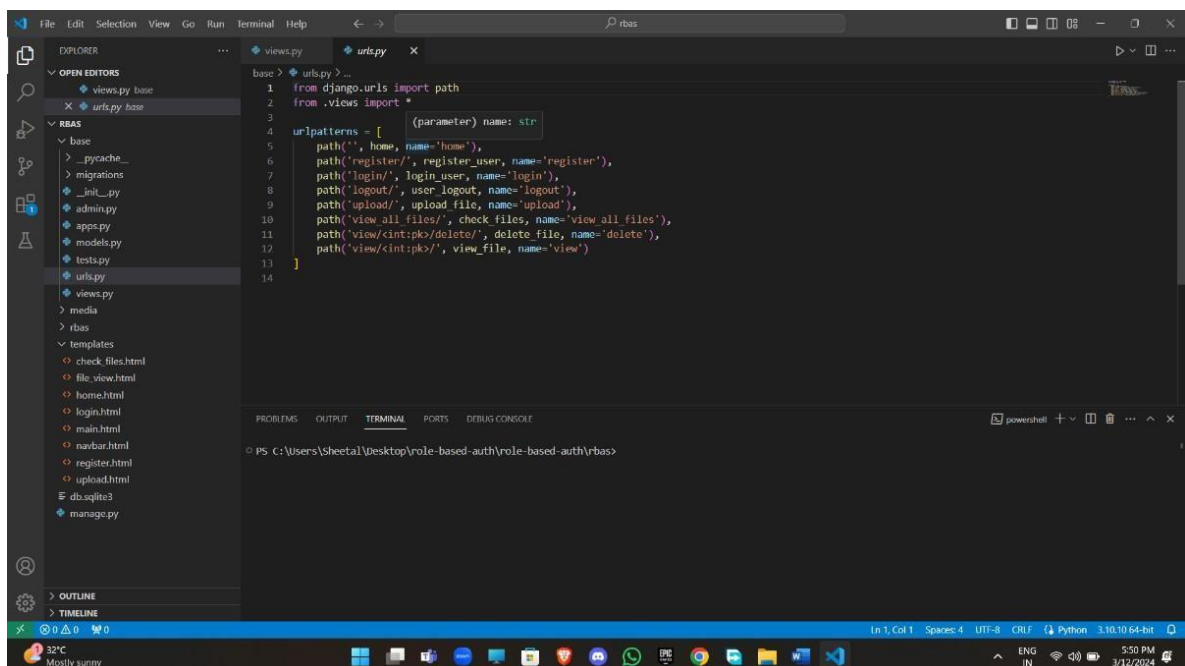
CHAPTER 6

RESULTS AND CONCLUSION

Enhancing security measures and reducing unauthorized access attempts need the implementation of a strong architecture for access control and identity management. Such a solution reduces the risk of data breaches and illegal use by ensuring that only authorized users can access resources and digital assets.

The creation of a thorough access control policy that outlines the guidelines and requirements for granting and revoking access permissions is the first step in putting this framework into action. This policy should outline requirements for user authentication, access permissions, and authorization levels. As a result, putting in place a solid architecture for identity management and access control is essential to boosting security measures and thwarting illegal access attempts to guarantee that only authorized users have access to critical data or resources.

The next step is to set up a centralized identity management system to control user identities and access rights. To guarantee that access privileges are suitable and current, this system should contain capabilities like user provisioning, role-based access control, and user lifecycle management. To increase the security of user credentials, the framework should additionally support multi-factor authentication techniques.



The screenshot shows a code editor with a file explorer on the left and a code editor on the right. The file explorer shows a project structure with folders like 'base', 'media', 'templates', and files like 'urls.py', 'views.py', 'models.py', 'tests.py', 'manage.py', 'db.sqlite3', 'register.html', 'upload.html', 'login.html', 'home.html', 'file.view.html', 'check_files.html', 'navbar.html', 'main.html', 'admin.py', 'migrations', and 'pycache'. The code editor shows the content of 'urls.py' with the following code:

```
1 from django.urls import path
2 from .views import *
3
4 urlpatterns = [
5     path('', home, name='home'),
6     path('register/', register_user, name='register'),
7     path('login/', login_user, name='login'),
8     path('logout/', user_logout, name='logout'),
9     path('upload/', upload_file, name='upload'),
10    path('view all files/', check_files, name='view all files'),
11    path('view/<int:pk>/delete/', delete_file, name='delete'),
12    path('view/<int:pk>/', view_file, name='view')
13 ]
14
```

The terminal at the bottom shows the command: `PS C:\Users\Sheetal\Desktop\role-based-auth\role-based-auth> rbas`

Fig 6.1 source code 1

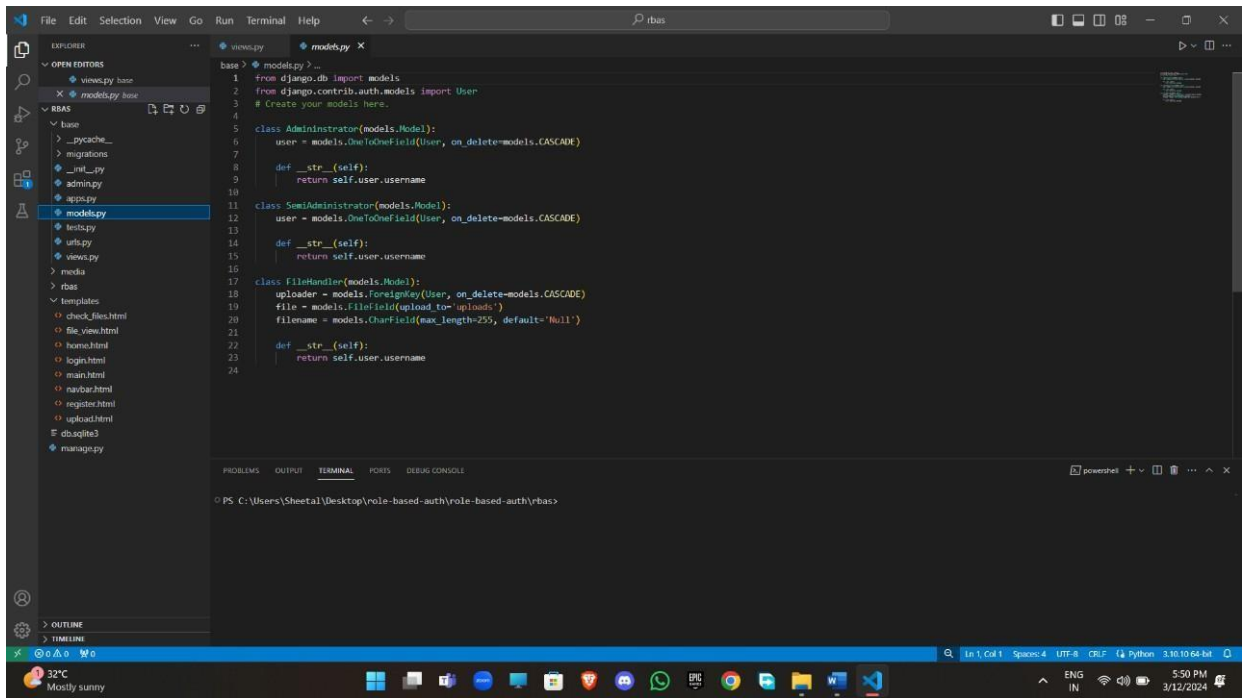


Fig 6.2 source code 2

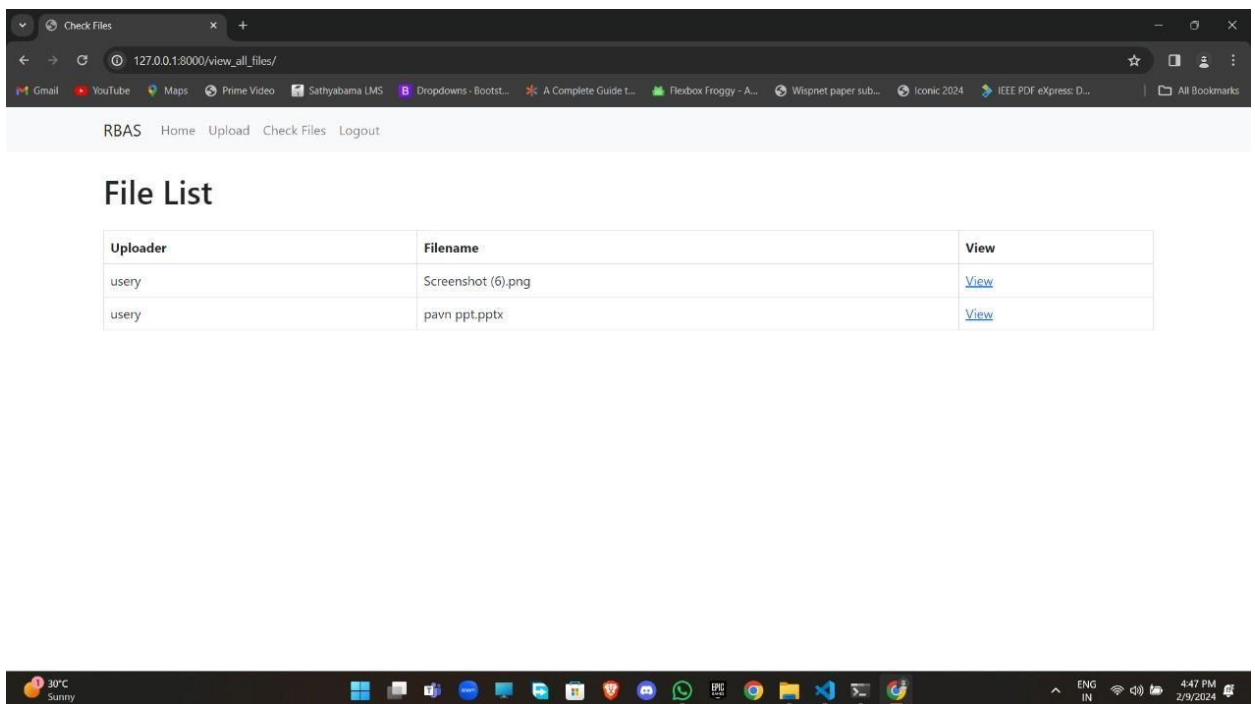


Fig 6.3 Files stored

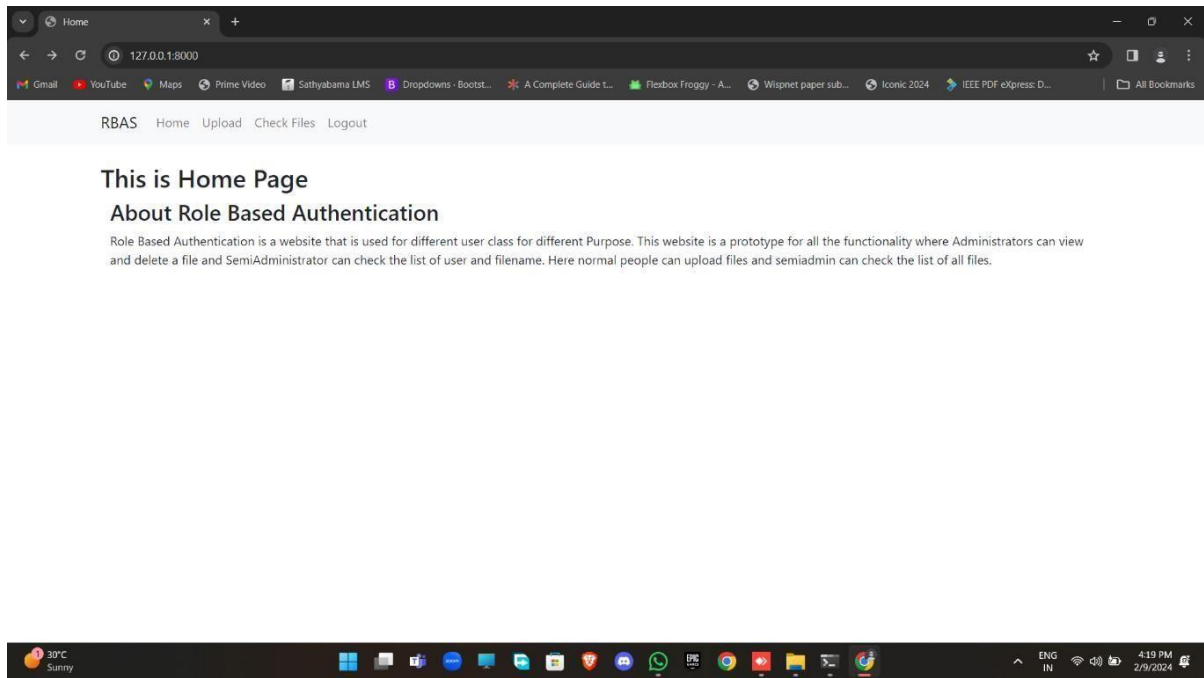


Fig 6.4 Rbas home page

The system should include a variety of authentication techniques such multi- factor authentication, biometrics, and secure credentials. To successfully manage user permissions and prevent privilege escalation, role-based access control and often updated policies should be put in place.

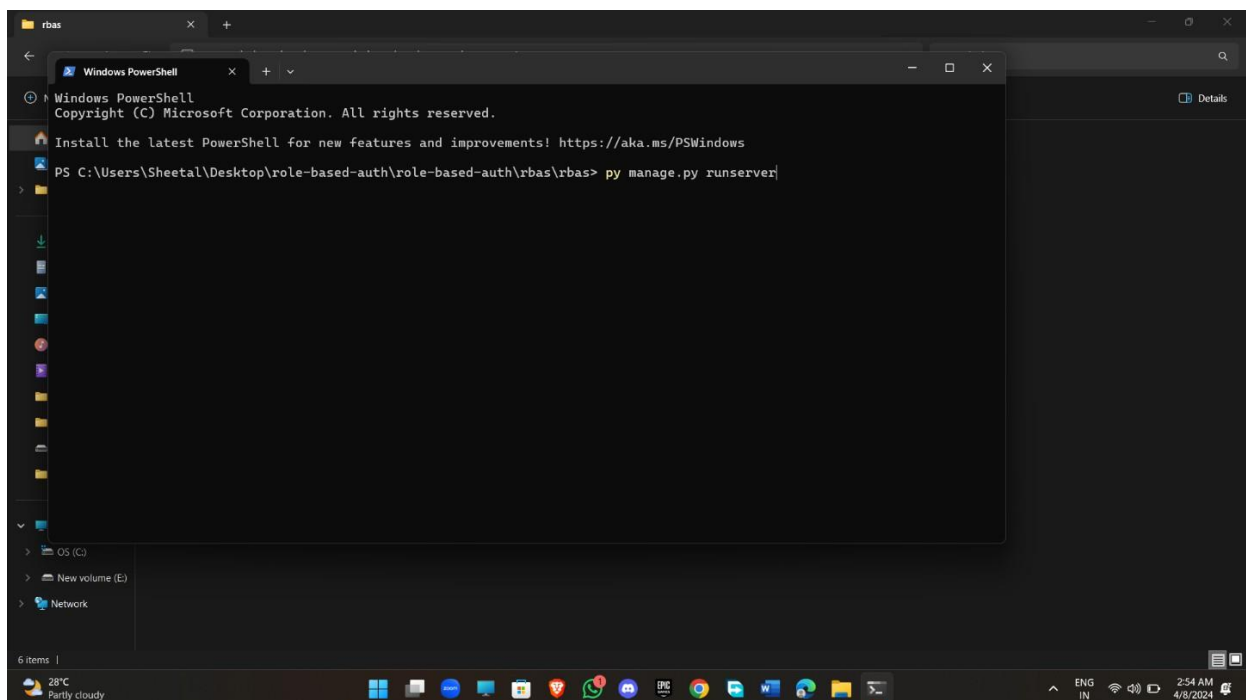


Fig 6.5 Server execution

Moreover, ongoing logging, monitoring, and access pattern analysis enable rapid detection of any suspect activity. Organizations can dramatically improve their security posture, safeguard sensitive data.

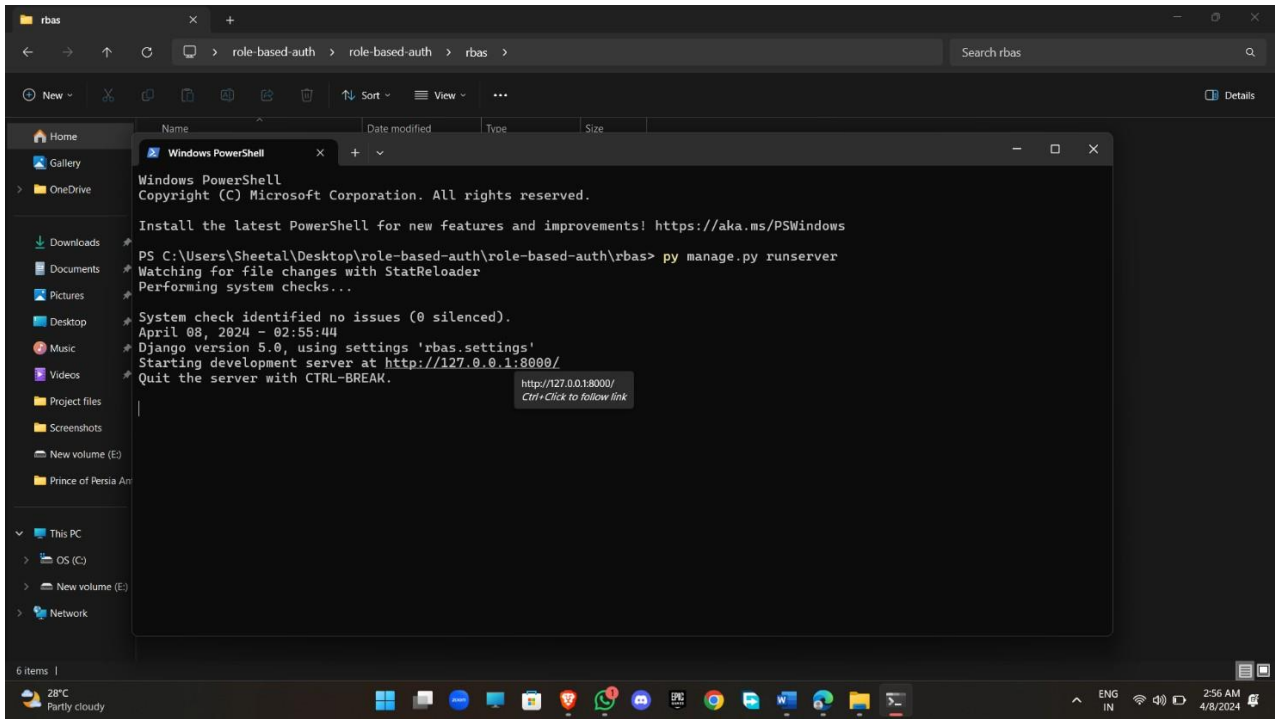


Fig 6.6 Server online

REFERENCES

- [1] Judge, M. A., Khan, A., Manzoor, A., & Khattak, H. A. (2022). Overview of smart grid implementation: Frameworks, impact, performance and challenges. *Journal of Energy Storage*, 49, 104056.
- [2] Kamble, S. S., Gunasekaran, A., Parekh, H., Mani, V., Belhadi, A., & Sharma, R. (2022). Digital twin for sustainable manufacturing supply chains: Current trends, future perspectives, and an implementation framework. *Technological Forecasting and Social Change*, 176, 121448.
- [3] Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., ... & Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. *Sensors*, 22(2), 572.
- [4] Qahtan, S., Sharif, K. Y., Zaidan, A. A., Alsattar, H. A., Albahri, O. S., Zaidan, B. B., ... & Mohammed, R. T. (2022). Novel multi security and privacy benchmarking framework for blockchain-based IoT healthcare industry 4.0 systems. *IEEE Transactions on Industrial Informatics*, 18(9), 6415-6423.
- [5] Damschroder, L. J., Reardon, C. M., Widerquist, M. A. O., & Lowery, J. (2022). The updated Consolidated Framework for Implementation Research based on user feedback. *Implementation science*, 17(1), 1-16.
- [6] Mahum, R., Munir, H., Mughal, Z. U. N., Awais, M., Sher Khan, F., Saqlain, M., ... & Tlili, I. (2023). A novel framework for potato leaf disease detection using an efficient deep learning model. *Human and Ecological Risk Assessment: An International Journal*, 29(2), 303-326.
- [7] Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). A Model-Driven Approach for Online Banking Application Using AngularJS Framework. *American Journal of Information Science and Technology*, 6(3), 52-63.
- [8] Khan, A. A., Wagan, A. A., Laghari, A. A., Gilal, A. R., Aziz, I. A., & Talpur, B. A. (2022). BloMT: A state-of-the-art consortium serverless network architecture for healthcare system using blockchain smart contracts. *IEEE Access*, 10, 78887- 78898.
- [9] Brazeau, N. F., Verity, R., Jenks, S., Fu, H., Whittaker, C., Winskill, P., ... & Okell, L. C. (2022). Estimating the COVID-19 infection fatality ratio accounting for sero reversion using statistical modelling. *Communications medicine*, 2(1), 54.

[10] Mahajan, H. B., Rashid, A. S., Junnarkar, A. A., Uke, N., Deshpande, S. D., Futane, P. R., ... & Alhayani, B. (2023). Integration of Healthcare 4.0 and blockchain into secure cloud- based electronic health records systems. *Applied Nanoscience*, 13(3), 2329-2342.

APPENDIX

A. Source Code

Models.py

```
from django.db import models
```

```
from django.contrib.auth.models import User
```

```
# Create your models here.
```

```
class Admininstrator(models.Model):
```

```
    user = models.OneToOneField(User, on_delete=models.CASCADE)
```

```
    def __str__(self):
```

```
        return self.user.username
```

```
class SemiAdministrator(models.Model):
```

```
    user = models.OneToOneField(User, on_delete=models.CASCADE)
```

```
    def __str__(self):
```

```
        return self.user.username
```

```
class FileHandler(models.Model):
```

```
    uploader = models.ForeignKey(User, on_delete=models.CASCADE)
```

```
    file = models.FileField(upload_to='uploads')
```

```
    filename = models.CharField(max_length=255, default='Null')
```

```
    def __str__(self):
```

```
        return self.user.username
```

```

views.py

from django.shortcuts import render, redirect

from .models import Admininstrator, SemiAdministrator, FileHandler

from django.contrib.auth.models import User

from django.contrib.auth import login, authenticate, logout

from django.http import HttpResponse

# Create your views here.

def home(request):

return render(request, 'home.html')


def register_user(request):

if request.method == 'POST':

username = request.POST['username']

password = request.POST['password']

flag = request.POST['flag']

user = User.objects.create(username = username, password = password)

user.save()

if flag == "1":

admin_instance = Admininstrator.objects.create(user = user)

admin_instance.save()

elif flag == "2":

semi_admin_instance = SemiAdministrator.objects.create(user=user)

semi_admin_instance.save()

else:

pass

login(request, user)

return redirect('home')

return render(request, 'register.html')

```

```

def login_user(request):
    if request.method == 'POST':
        username = request.POST['username']
        password = request.POST['password']
        user = authenticate(request, username=username, password=password)
        if user is not None:
            login(request, user)
            return redirect('home')
        return render(request, 'login.html')
    def user_logout(request):
        logout(request)
        return redirect('home')

    def upload_file(request):
        context = {}
        if request.method == 'POST':
            curr_user = request.user
            file = request.FILES['file']
            filename = file.name
            file_handle = FileHandler(uploader = curr_user, file=file, filename = filename)
            file_handle.save()
            return redirect('home')
        return render(request, 'upload.html', context)

```

```

def check_files(request):

    context = {}

    curr_user = request.user

    try:

        is_admin = Admininstrator.objects.get(user=curr_user)

    except :

        is_admin = Nonetry:

        is_semiAdmin = SemiAdministrator.objects.get(user=curr_user)

    except :

        is_semiAdmin = None

    context['files'] = []

    if is_admin or is_semiAdmin:

        all_file_ins = FileHandler.objects.all()for

        file in all_file_ins:

            context['files'].append({'id' :

            file.id,

            'uploader' : file.uploader.username, 'filename'

            : file.filename

            })

    return render(request, 'check_files.html', context) return

HttpResponse('User isnt Admin or Semi Admin')

def delete_file(request, pk)

curr_user = request.usertry:

is_admin = Admininstrator.objects.get(user=curr_user)

```

```

except:
is_admin = Noneif
is_admin:
file_ins = FileHandler.objects.get(id=pk)
file_ins.delete()
return redirect('view_all_files')
return HttpResponseRedirect('User is not Admin')

def view_file(request
pk):context = {}
curr_user = request.user
is_admin = Admininstrator.objects.get(user=curr_user)
if is_admin:
file_ins = FileHandler.objects.get(id=pk)
context['file'] = {
'id' : file_ins.id,
'filename' : file_ins.filename,
'file_url' : file_ins.file.url,
}
print(context)
return render(request, 'file_view.html', context)
return HttpResponseRedirect('User is not Admin')

urls.py
from django.urls import
pathfrom .views import *
urlpatterns = [

```

```

path("", home, name='home'),
path('register/', register_user, name='register'),
path('login/', login_user, name='login'),
path('logout/', user_logout, name='logout'),
path('upload/', upload_file, name='upload'),
path('view_all_files/', check_files, name='view_all_files'),
path('view/<int:pk>/delete/', delete_file, name='delete'),
path('view/<int:pk>', view_file, name='view')
]

```

Settings.py

"""

Django settings for rbas project.

Generated by 'django-admin start project' using Django 4.2.2.

For more information on this file, see

<https://docs.djangoproject.com/en/4.2/topics/settings/>

For the full list of settings and their values, see

<https://docs.djangoproject.com/en/4.2/ref/settings/>

"""

```

from pathlib import Path

```

```

import os

```

```

# Build paths inside the project like this: BASE_DIR / 'subdir'.

```

```

BASE_DIR = Path(__file__).resolve().parent.parent

```

```

# Quick-start development settings - unsuitable for production

# See https://docs.djangoproject.com/en/4.2/howto/deployment/checklist/


# SECURITY WARNING: keep the secret key used in production secret!
SECRET_KEY = 'django-insecure-yb=92rg!22#j^i&0zr5hz&ggw@@j_^f3in@jx&)v0i))ss0ybl'


# SECURITY WARNING: don't run with debug turned on in production!
DEBUG = True


ALLOWED_HOSTS = []


# Application definition


INSTALLED_APPS = [
'django.contrib.admin',
'django.contrib.auth',
'django.contrib.contenttypes',
'django.contrib.sessions',
'django.contrib.messages',
'django.contrib.staticfiles', 'base'
]


MIDDLEWARE = [
'django.middleware.security.SecurityMiddleware',

```

```
'django.contrib.sessions.middleware.SessionMiddleware',  
'django.middleware.common.CommonMiddleware',  
'django.middleware.csrf.CsrfViewMiddleware',  
'django.contrib.auth.middleware.AuthenticationMiddleware',  
'django.contrib.messages.middleware.MessageMiddleware',  
'django.middleware.clickjacking.XFrameOptionsMiddleware',  
]
```

```
ROOT_URLCONF = 'rbas.urls'
```

```
TEMPLATES = [  
    {  
        'BACKEND': 'django.template.backends.django.DjangoTemplates',  
        'DIRS': ['templates'],  
        'APP_DIRS': True,  
        'OPTIONS': {  
            'context_processors': [  
                'django.template.context_processors.debug',  
                'django.template.context_processors.request',  
                'django.contrib.auth.context_processors.auth',  
                'django.contrib.messages.context_processors.messages',  
            ],  
        },  
    },  
]  
]
```

```
WSGI_APPLICATION = 'rbas.wsgi.application'
```

Database

<https://docs.djangoproject.com/en/4.2/ref/settings/#databases>

```
DATABASES = {  
    'default': {  
        'ENGINE': 'django.db.backends.sqlite3',  
        'NAME': BASE_DIR / 'db.sqlite3',  
    }  
}
```

Password validation

<https://docs.djangoproject.com/en/4.2/ref/settings/#auth-password-validators>

```
AUTH_PASSWORD_VALIDATORS = [  
    {  
        'NAME': 'django.contrib.auth.password_validation.UserAttributeSimilarityValidator',  
    },  
    {  
        'NAME': 'django.contrib.auth.password_validation.MinimumLengthValidator',  
    },  
    {  
        'NAME': 'django.contrib.auth.password_validation.CommonPasswordValidator',  
    },  
    {  
        'NAME': 'django.contrib.auth.password_validation.NumericPasswordValidator',  
    },  
]
```

Internationalization

<https://docs.djangoproject.com/en/4.2/topics/i18n/>

LANGUAGE_CODE = 'en-us'

TIME_ZONE = 'UTC'

USE_I18N = True

USE_TZ = True

Static files (CSS, JavaScript, Images)

<https://docs.djangoproject.com/en/4.2/howto/static-files/>

STATIC_URL = 'static/'

MEDIA_URL = '/media/'

MEDIA_ROOT = os.path.join(BASE_DIR, 'media')

X_FRAME_OPTIONS = 'SAMEORIGIN'

Default primary key field type

<https://docs.djangoproject.com/en/4.2/ref/settings/#default-auto-field>

DEFAULT_AUTO_FIELD = 'django.db.models.BigAutoField'

Wsgi.py

.....

WSGI config for rbas project.

It exposes the WSGI callable as a module-level variable named ``application``.

For more information on this file, see

<https://docs.djangoproject.com/en/4.2/howto/deployment/wsgi/>

.....

```
import os
```

```
from django.core.wsgi import get_wsgi_application
```

```
os.environ.setdefault('DJANGO_SETTINGS_MODULE', 'rbas.settings')
```

```
application = get_wsgi_application()
```

asgi.py

.....

ASGI config for rbas project.

It exposes the ASGI callable as a module-level variable named ``application``.

For more information on this file, see

<https://docs.djangoproject.com/en/4.2/howto/deployment/asgi/>

.....

```
import os
```

```
from django.core.asgi import get_asgi_application
```

```
os.environ.setdefault('DJANGO_SETTINGS_MODULE', 'rbas.settings')
```

```
application = get_asgi_application()
```

```
admins.py
```

```
from django.contrib import admin
```

```
from .models import Admininstrator, SemiAdministrator, FileHandler
```

```
# Register your models here.
```

```
admin.site.register(Admininstrator)
```

```
admin.site.register(SemiAdministrator)
```

```
admin.site.register(FileHandler)
```

```
check files.html
```

```
{% extends 'main.html' %}
```

```
{% block title %}Check Files{% endblock title %}
```

```
{% block content %}
```

```
<div class="container mt-4">
```

```
<h1 class="mb-4">File List</h1>
```

```
<div>
```

```
{% if files %}
```

```
<table class="table table-bordered">
```

```
<thead>
```

```
<tr>
```

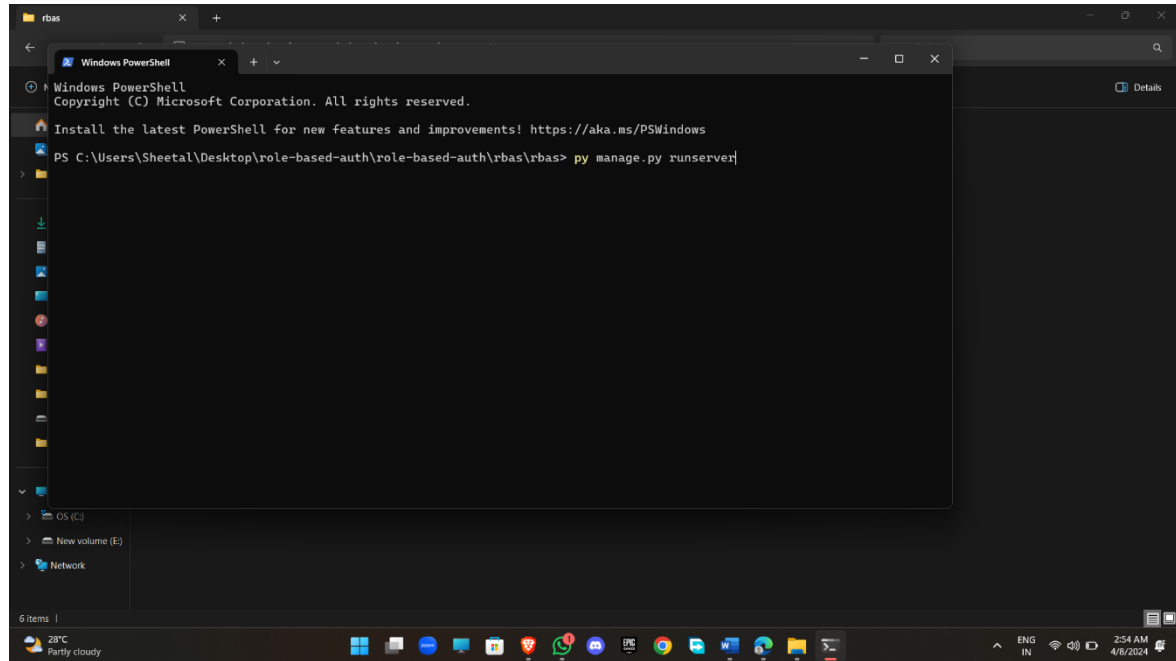
```

<th>Uploader</th>
<th>Filename</th>
    <th>View</th>
</tr>
</thead>
<tbody>
{% for file in files %}
<tr>
<td>{{ file.uploader }}</td>
<td>{{ file.filename }}</td>
<td><a href="{% url 'view' file.id %}">View</a></td>
</tr>
{% endfor %}
</tbody>
</table>
{% else %}
<p>No files available</p>
{% endif %}
</div>
</div>
{% endblock content %}
Login.html
{% extends 'main.html' %}
{% block title %}User Login{% endblock title %}
{% block content %}
<div class="container mt-4">
<form method="POST">

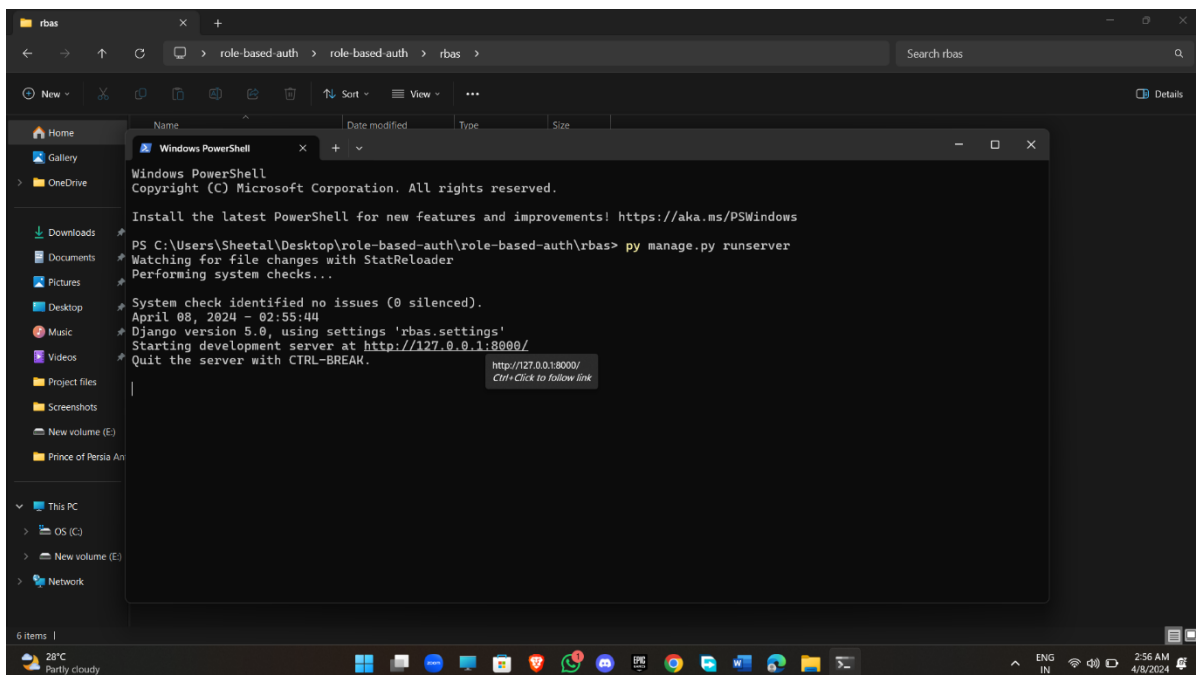
```

```
{% csrf_token %}
<label class="form-label">Username</label>
<input type="text" name="username" class="form-control" />
<label class="form-label">Password</label>
<input type="password" name="password" class="form-control"/>
<button type="submit" class="btn btn-primary">Login</button>
</form>
</div>
{% endblock content %}
```

B. SCREENSHOTS



B.1 Executing server



B.2 Running Code

```
base > models.py > ...
1 from django.db import models
2 from django.contrib.auth.models import User
3 # Create your models here.
4
5 class Administrator(models.Model):
6     user = models.OneToOneField(User, on_delete=models.CASCADE)
7
8     def __str__(self):
9         return self.user.username
10
11 class SemiAdministrator(models.Model):
12     user = models.OneToOneField(User, on_delete=models.CASCADE)
13
14     def __str__(self):
15         return self.user.username
16
17 class FileHandler(models.Model):
18     uploader = models.ForeignKey(User, on_delete=models.CASCADE)
19     file = models.FileField(upload_to='uploads')
20     filename = models.CharField(max_length=255, default='Null')
21
22     def __str__(self):
23         return self.user.username
24
```

PROBLEMS OUTPUT TERMINAL PORTS DEBUG CONSOLE

PS C:\Users\Sheetal\Desktop\role-based-auth\role-based-auth> rbas

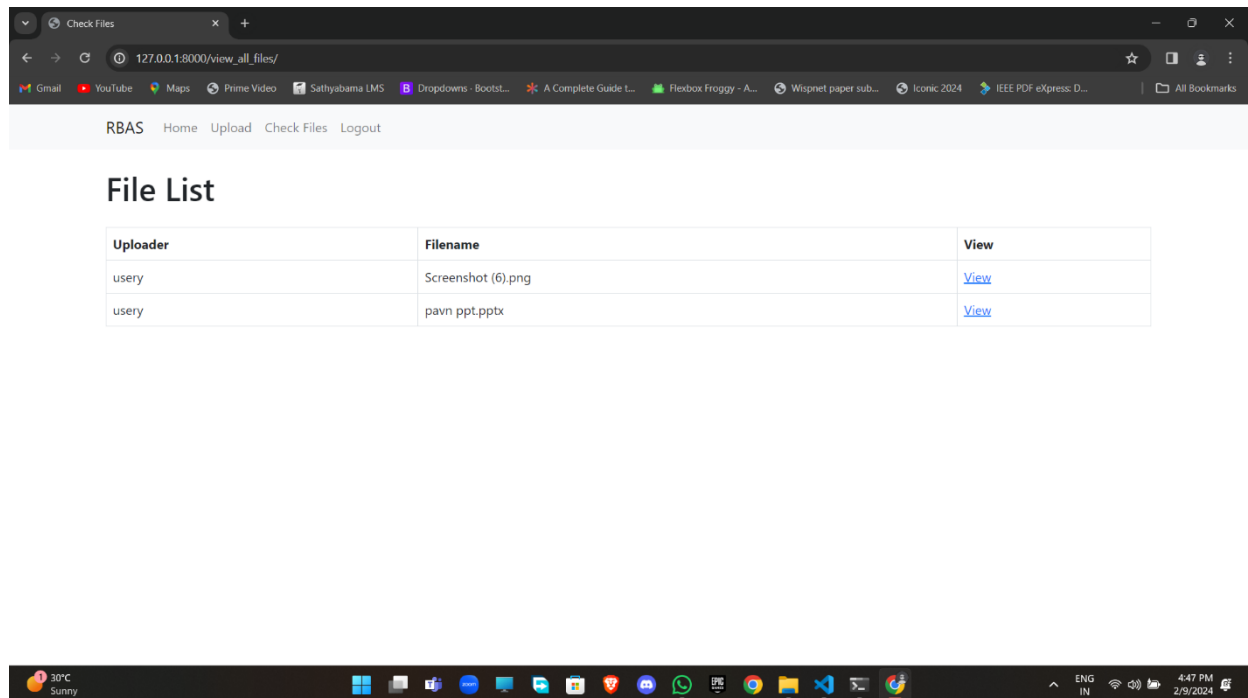
B.3 Models Code

```
base > urls.py > ...
1 from django.urls import path
2 from .views import *
3
4 urlpatterns = [
5     path('', home, name='home'),
6     path('register/', register_user, name='register'),
7     path('login/', login_user, name='login'),
8     path('logout/', user_logout, name='logout'),
9     path('upload/', upload_file, name='upload'),
10    path('view_all_files/', check_files, name='view_all_files'),
11    path('view/cint:pk/delete/', delete_file, name='delete'),
12    path('view/cint:pk/', view_file, name='view')
13 ]
14
```

PROBLEMS OUTPUT TERMINAL PORTS DEBUG CONSOLE

PS C:\Users\Sheetal\Desktop\role-based-auth\role-based-auth> rbas

B.4 Urls Code



B.5 File list

C. RESEARCH PAPER

Implementing a Robust Framework for Access Control and Identity Management in order to Enhance Security Measures and Mitigate Unauthorized Access Attempts.

KSRM Sheetal¹, Ballapuram Yogesheshwar², Jemshia Miriam*

Sathyabama Institute of Science and Technology, Jeppiaar Nagar, SH 49A, 600119, Tamil Nadu

Corresponding Author : jemshia.cse@sathyabama.ac.in

ABSTRACT

This article recommends the development of a robust framework for access control and identity management in order to increase security precautions and decrease unauthorized access attempts. The increased reliance on digital systems and networks has made security a primary concern for both organizations and consumers. It has been demonstrated that traditional user IDs and password-based access control systems are poor at protecting sensitive information and thwarting unauthorized access. To ensure the integrity and confidentiality of data, a comprehensive architecture with many security levels is required. The proposed framework makes use of cutting-edge technology, such as biometrics, multi-factor authentication, and encryption, to build a more dependable and resilient system. It also uses proactive monitoring and threat detection techniques to quickly identify potential security breaches and take the necessary action. Moreover, the framework includes a centralized identity management system that manages user profiles, access privileges, and authentication information, enabling efficient management of user access rights and permissions. By implementing this strategy, organizations can significantly strengthen their security posture, thwart unauthorized access attempts, and safeguard critical data. This research contributes to the subject of access control and identity management by providing a comprehensive framework that combines several security methods to create a strong defense against potential attacks.

Keywords: *access control, identity management, security measures, unauthorized access, robust framework, biometrics, multi-factor authentication, encryption, threat detection, centralized identity management, user access rights, proactive monitoring.*

I. INTRODUCTION

It is crucial to put in place a solid framework for access control and identity management in the present digital world, where security risks are continually evolving and getting more complex. As businesses rely more on digital systems and networks, they run the danger of unwanted access attempts, which might lead to data breaches, information theft, and other undesirable effects.

To improve security measures and reduce illegal access attempts, a comprehensive approach that goes beyond simple user authentication is required. A strong access control framework incorporates a combination of technologies, policies, and procedures to ensure that only authorized individuals can access sensitive resources and perform allowed tasks. Together with user access, this framework should also include hardware, software, and other elements of the IT infrastructure.

A robust access control framework is built on the usage of strong authentication mechanisms. Passwords are no longer sufficient on their own because they are so readily cracked.

Multi-factor authentication (MFA) adds an additional layer of protection by asking users to submit multiple forms of identity, such as a password, an SMS code, or a fingerprint.

As a result, the danger of unwanted access attempts is significantly reduced because it takes several authentication elements to fool the system.

The identity management component of the access control architecture is crucial since it ensures that only those with the proper authorization have access capabilities. This requires the creation and management of user accounts, the establishment of user roles and permissions, and the routine review and updating of access privileges in accordance with the principle of least privilege. By using a centralized identity management system, organizations can efficiently track and control user access across various systems and applications. As a result, there is a lower possibility of unwanted access brought on by forgotten user accounts or outdated permissions.

In addition to authentication and identity management, access control policies and procedures should be designed to define and enforce the appropriate access controls depending on organizational needs and regulatory compliance. This involves abiding by the least privilege principle, which states that users should only be granted the bare minimum of access necessary to perform their job responsibilities. Regular access reviews and audits should be performed to find and eliminate unneeded privileges, limit the attack surface, and lessen the risk of unwanted access attempts.

To put in place a solid framework for access control and identity management, IT departments, security teams, and end users must collaborate holistically. To assist them in comprehending the need for safe access procedures and the potential consequences associated with unauthorized access attempts, employees should receive proper training and awareness programs. In order to detect suspicious activity in real-time and take

appropriate action, access logs should be regularly watched and analyzed. This will enable businesses to proactively lower security risks.

II. RELATED WORKS

1. This study proposes a framework that combines traditional access control methods with advanced technologies such as biometrics and multi-factor authentication. The framework focuses on the enforcement of security policies and the prevention of unauthorized access attempts.

2. A literature review highlighted the importance of context-aware access control systems in enhancing security measures. The study suggested incorporating contextual information, such as user location and time, into the access control decision-making process to improve system effectiveness.

3. An empirical study examined the effectiveness of role-based access control (RBAC) in mitigating unauthorized access attempts. The research findings indicated that RBAC reduces the risk of unauthorized access by providing fine-grained access control based on predefined roles and responsibilities.

4. This article discussed the challenges of implementing a robust access control framework in cloud computing environments. The study emphasized the need for scalable and flexible access control mechanisms to address the dynamic nature of cloud-based systems.

5. A survey of existing access control models highlighted the importance of managing user identities efficiently to enhance security measures. The study

suggested adopting identity management systems that integrate with access control mechanisms to provide a holistic approach to security.

6. This research examined the role of machine learning algorithms in enhancing access control systems. The study proposed using anomaly detection techniques to identify and mitigate unauthorized access attempts in real-time.

7. An analysis of access control frameworks in IoT (Internet of Things) environments revealed the need for scalable and adaptable access control mechanisms to accommodate the large number of interconnected devices. The study recommended utilizing attribute-based access control (ABAC) for IoT security.

8. This study explored the challenges associated with managing access control and identity management in distributed systems. The research findings emphasized the importance of a centralized policy management system to ensure consistent access control across multiple entities.

9. A review of access control mechanisms in healthcare systems highlighted the unique requirements and challenges faced in this domain. The study suggested implementing a robust access control framework that considers patient privacy, role-based access, and audit logging.

10. This literature survey discussed the role of blockchain technology in enhancing access control and identity management. The study proposed utilizing blockchain for decentralized and tamper-proof identity verification, reducing the risk of unauthorized access attempts.

III. EXISTING SYSTEM

The current access control and identity

management system may have a number of drawbacks that make it difficult to strengthen security precautions and reduce illegal access attempts. First off, the absence of a solid structure is one of the system's biggest flaws. This implies that the system could not have a complete set of guidelines and regulations to control access to resources. Without a solid framework, it is challenging to establish and implement appropriate access restrictions, which can result in unauthorized people getting access to confidential data or resources.

The lack of centralized management is yet another drawback of the current system. It can be difficult to maintain a cohesive and streamlined strategy when access control and identity management functions are spread out over numerous systems and platforms. Lack of centralization may make it difficult to track user activity and apply access limits consistently.

Moreover, the scalability and adaptability of the current technology might not be adequate. The system should be able to adjust as organizations expand and their needs alter. Yet, a rigid system could find it difficult to adapt to changing demands, creating inefficiencies and weaknesses. Similar to this, the current system might not have the necessary integration capabilities, making it difficult to integrate with other security tools and systems. This can impair the capacity to identify and react to illegal access attempts as well as the overall efficacy of security measures.

Also, the current approach may make user provisioning and deprovisioning processes time-consuming and error-prone. It can be slower and more error-prone to manually manage user accounts and access privileges, which makes it simpler for unauthorized users to exploit weaknesses. Also, the current system can use outmoded or constrained authentication techniques, including passwords that are too simple or

don't use multiple factors. Attackers looking to gain unauthorized access may take advantage of these flaws.

Last but not least, the current system could not have reliable auditing and monitoring capabilities. Tracking and looking into unauthorized or questionable activity is challenging without thorough logging and monitoring features. This makes it harder to implement appropriate security measures and react quickly to threats.

In conclusion, the shortcomings of the current access control and identity management system make it difficult to improve security precautions and reduce unwanted access attempts. Inadequate framework, lack of centralized management, scalability and flexibility concerns, restricted integration capabilities, time-consuming user provisioning procedures, antiquated authentication techniques, and insufficient auditing and monitoring functionality are some of these drawbacks. Establishing a more reliable and efficient access control and identity management system requires addressing these issues.

IV. PROPOSED SYSTEM

The proposed work intends to develop a strong framework for identity management and access control in order to strengthen security precautions and reduce illegal access attempts. The main goals of this work are to gain a thorough understanding of access control and identity management principles, to analyze the system architecture currently in place and identify any potential security holes, to design and implement secure authentication and authorization mechanisms, and to assess the efficacy of the suggested framework.

The study will start with a thorough examination of access control and identity management principles and best practices in order to accomplish these goals. To create a strong theoretical foundation, this

will entail researching pertinent literature, standards, and guidelines.

The current system architecture will then be examined to find any potential flaws or vulnerabilities in the access control systems already in place. Examining user roles and rights, password guidelines, and user management procedures are all part of this process. In order to create effective defenses, prospective attack vectors like brute-force attacks or efforts at privilege escalation will also be taken into account.

A solid framework for access control and identity management will be created and put into place based on the analysis. To guarantee that only authorized users may access the system, this framework will contain user authentication techniques like multi-factor authentication or biometric authentication. To manage user permissions and limit unwanted access attempts, role-based access control (RBAC) or attribute-based access control (ABAC) techniques will also be used.

To ensure the security and effectiveness of the framework, thorough testing and validation will be done during the installation phase. To do this, multiple attack scenarios will be simulated, and the system's capacity to identify and thwart unauthorized access attempts will be assessed. To maximize the effectiveness of the framework, performance indicators like reaction time and resource use will also be tracked.

The success of the framework will then be assessed in comparison to pre-established security criteria and industry best practices. The framework will be improved in accordance with the results of this review in order to fill up any gaps or areas for improvement.

In order to strengthen security measures and reduce illegal access attempts, the proposed work would develop a strong

framework for access control and identity management. This work will assist in enhancing the security posture of the system and guarantee the confidentiality, integrity, and availability of priceless resources by developing a thorough understanding of access control principles, analyzing the architecture of the current system, designing and implementing secure mechanisms, and evaluating the effectiveness of the framework.

V. SYSTEM ARCHITECTURE

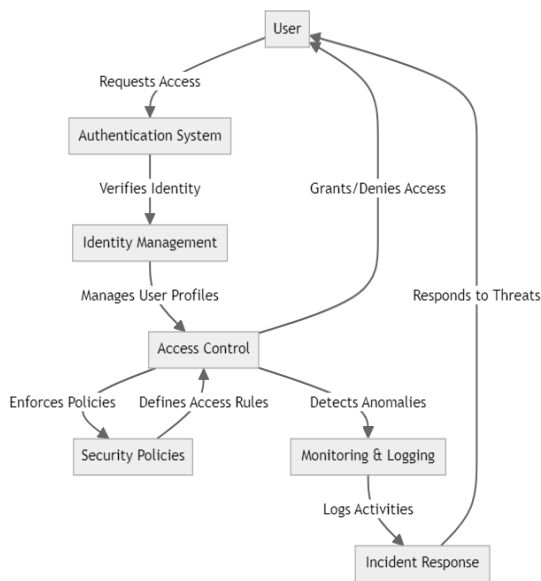


Fig. 1. System Architecture

VI. METHODOLOGY

1. **Authentication Module:** An effective framework for access control and identity management must include a strong authentication module. Its major objective is to confirm the legitimacy of users trying to access the system and make sure that only people with permission are given access. To strengthen security measures, this module often incorporates a variety of authentication techniques including passwords, biometrics, or multi-factor authentication. In order to reduce illegal access attempts, it also includes features like password rules (such as minimum length and complexity requirements) and account lockout procedures. To simplify the user experience without compromising

security, the authentication module may also incorporate features like session management and single sign-on.

2. **Authorization Module:** The authorization module is in charge of figuring out the rights of authorized users to access certain resources. According to their given responsibilities or permissions, it implements access control policies that specify what resources or actions a user is permitted to access. The potential harm brought on by unauthorized access attempts is minimized by this module, which makes sure that users can only carry out tasks or access resources that are required for their job obligations. Granular access control should be supported by the authorization module, enabling administrators to specify fine-grained permissions at various system levels. In order to provide flexibility and scalability in managing access privileges, it should also incorporate features like role-based access control (RBAC) and attribute-based access control (ABAC).

3. **Auditing and Monitoring Module:** This module is essential for boosting security protocols and spotting illegal access attempts. It monitors user activity, logs events, and produces logs that may be examined to spot any unusual behavior or security lapses. Real-time monitoring, anomaly detection, and alarm systems should all be included in this module in order to quickly identify and stop unwanted access attempts. Additionally, it should offer thorough reporting capabilities so that system administrators may examine access patterns, spot potential security holes, and create compliance reports for auditing needs. In order to combine logs and enable centralized monitoring and analysis, the auditing and monitoring module should also support integration with security information and event management (SIEM) systems.

The suggested solution can greatly improve security measures and reduce unauthorized access attempts by integrating these three modules—authentication, authorization, and auditing & monitoring—into a strong framework for access control and identity management. Together, these modules validate user identities, implement access control rules, and keep an eye on user behavior to make sure that only authorized users have access privileges and that any unauthorized access attempts are quickly identified and dealt with.

VII. RESULT AND DISCUSSION

Enhancing security measures and reducing unauthorized access attempts need the implementation of a strong architecture for access control and identity management. Such a solution reduces the risk of data breaches and illegal use by ensuring that only authorized users can access resources and digital assets.

The creation of a thorough access control policy that outlines the guidelines and requirements for granting and revoking access permissions is the first step in putting this framework into action. This policy should outline requirements for user authentication, access permissions, and authorization levels.

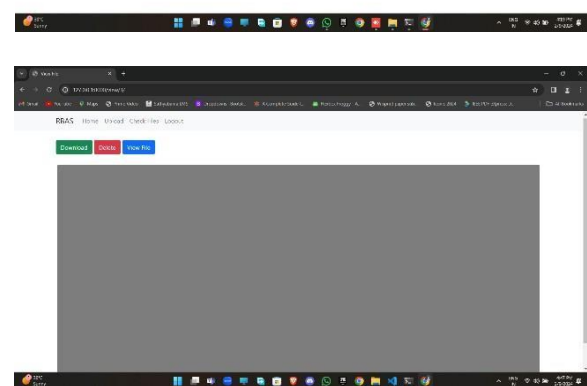
The next step is to set up a centralized identity management system to control user identities and access rights. To guarantee that access privileges are suitable and current, this system should contain capabilities like user provisioning, role-based access control, and user lifecycle management. To increase the security of user credentials, the framework should additionally support multi-factor authentication techniques.

In order to detect any suspicious activity or unauthorized access attempt in real-time, the system should also include continuous monitoring and auditing capabilities. This

involves keeping an eye on login processes, access requests, and modifications to access rights. Access log audits on a regular basis can assist find potential security holes and guarantee regulatory compliance.

The architecture should incorporate tools for access control enforcement, such as firewalls, intrusion detection systems, and encryption, to further strengthen security measures. These technologies can shield confidential information from breaches into networks and guard against unwanted access. To find and fix any system flaws, regular vulnerability analyses and penetration tests should also be carried out.

Ultimately, putting in place a strong framework for identity management and access control is crucial for preserving the privacy, availability, and integrity of digital assets. Organizations can improve their security measures and successfully reduce unauthorized access attempts by adhering to these recommendations and keeping the system updated..



VIII. CONCLUSION

As a result, putting in place a solid architecture for identity management and access control is essential to boosting security measures and thwarting illegal access attempts. To guarantee that only authorized users have access to critical data or resources, the system should include a variety of authentication techniques such as multi-factor authentication, biometrics, and secure credentials. To successfully manage user permissions and prevent privilege

escalation, role-based access control and often updated policies should be put in place. Moreover, ongoing logging, monitoring, and access pattern analysis enable rapid detection of any suspect activity. Organizations can dramatically improve their security posture, safeguard sensitive data, and lower the possibility of illegal access attempts by putting these steps in place.

IX. FUTURE WORK

There are a number of future works that can be identified in order to establish a strong framework for access control and identity management, improve security precautions, and mitigate illegal access attempts. First, a thorough examination of the system's flaws and vulnerabilities will reveal important information about what has to be improved. To strengthen user verification processes, this study can be followed by the creation of cutting-edge authentication techniques like multi-factor authentication or biometric authentication. Additionally, the application of attribute-based access control (ABAC) and role-based access control (RBAC) can effectively limit unwanted access and offer more granular control over user permissions. To quickly identify any anomalies or suspect activity, it is essential to continuously monitor and audit the access control system. The use of machine learning algorithms can improve this monitoring even further because they make it possible to spot patterns

and departures from norms. To find and fix any potential vulnerabilities, routine security evaluations and penetration tests should be carried out. Moreover, it is crucial to stay current with encryption techniques and secure credential technologies in order to maintain the system secure and resistant to new threats.

REFERENCES

- [1] X. Sun and X. Meng, "A Robust Control Approach to Event-Triggered Networked Control Systems With Time-Varying Delays," in *IEEE Access*, vol. 9, pp. 64653-64664, 2021, doi: 10.1109/ACCESS.2021.3075696.
- [2] Z. Ning, Y. Mao, Y. Huang and C. Gao, "Robust Current Control of Voice Coil Motor in Tip-Tilt Mirror Based on Disturbance Observer Framework," in *IEEE Access*, vol. 9, pp. 96814-96822, 2021, doi: 10.1109/ACCESS.2021.3057162.
- [3] I. Brahmia, J. Wang, H. Xu, H. Wang and L. D. O. Turci, "Robust Data Predictive Control Framework for Smart Multi-Microgrid Energy Dispatch Considering Electricity Market Uncertainty," in *IEEE Access*, vol. 9, pp. 32390-32404, 2021, doi: 10.1109/ACCESS.2021.3060315.
- [4] A. S. S. Ianagui, P. C. De Mello and E. A. Tannuri, "Robust Output-Feedback Control in a Dynamic Positioning System via High Order Sliding Modes: Theoretical Framework and Experimental Evaluation," in *IEEE Access*, vol. 8, pp. 91701-91724, 2020, doi: 10.1109/ACCESS.2020.2994515.
- [5] A. N. Doss, D. Shah, G. F. Smaisim, M. Olha and S. Jaiswal, "A Comprehensive Analysis of Internet of Things (IOT) in Enhancing Data Security for Better System Integrity - A Critical Analysis on the Security Attacks and Relevant Countermeasures," 2022 2nd International

Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 165-167, doi: 10.1109/ICACITE53722.2022.9823817.

[6] K. K. Karmakar, V. Varadharajan, U. Tupakula and M. Hitchens, "Towards a Dynamic Policy Enhanced Integrated Security Architecture for SDN Infrastructure," NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 2020, pp. 1-9, doi: 10.1109/NOMS47738.2020.9110405.

[7] M. Shabbir et al., "Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing," in IEEE Access, vol. 9, pp. 8820-8834, 2021, doi: 10.1109/ACCESS.2021.3049564.

[8] A. Salaria, C. Kumar and A. Mishra, "Security Intensification in Restricted Area By Confining Unauthorized Smart Phone Applications," 2022 International Conference on Futuristic Technologies (INCOFT), Belgaum, India, 2022, pp. 1-5, doi: 10.1109/INCOFT55651.2022.10094434.

[9] Y. S. Chaudhry, U. Sharma and A. Rana, "Enhancing Security Measures of AI Applications," 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2020, pp. 713-716, doi: 10.1109/ICRITO48877.2020.9197790.

[10] K. K. Karmakar, V. Varadharajan, U. Tupakula, S. Nepal and C. Thapa, "Towards a Security Enhanced Virtualised Network Infrastructure for Internet of Medical Things (IoMT)," 2020 6th IEEE Conference on Network Softwarization (NetSoft), Ghent, Belgium, 2020, pp. 257-261, doi: 10.1109/NetSoft48620.2020.9165387.

CONFERENCE CERTIFICATE

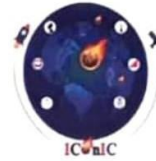


PANIMALAR ENGINEERING COLLEGE

An Autonomous Institution & Affiliated to Anna University, Chennai
Approved by AICTE, New Delhi, Accredited by National Board of Accreditation (NBA)
Approved by UGC for 2(f) & 12(B) Status
Bangalore Trunk Road, Poonamallee, Chennai-600123.



PECTEAM 2K24



This is to certify that Dr./Mr./Ms. KSRM SHEETAL of IVth YR CSE from
SCIENCE + TECHNOLOGY
SATHYABAMA INSTITUTE OF has presented paper entitled IMPLEMENTING ROBUSTER FRAMEWORK
FOR ACCESS CONTROL AND IDENTITY MANAGEMENT IN ORDER TO ENHANCE SECURITY MEASURES
AND MITIGATE UNAUTHORIZED ACCESS ATTEMPTS. in
7th International Conference on Intelligent Computing (ICoNIC) held on 22nd & 23rd MARCH, 2024.

FACULTY CO-ORDINATOR Prof. S. VIMALA, M.TECH., (Ph.D)

CO - CONVENER

CO - PATRON

Dr. K. MANI, M.E., Ph.D.,

