**SECURE DATA SHARING USING AN ELLIPTIC CURVE CRYPTOGRAPHY METHOD IN CLOUD COMPUTING**

**ABSTRACT**

The patient's medical history and prescription information are contained in electronic health records. The attackers are interested in the health records because they contain significant information. An incorrect medicine or operation is the result of a lost electronic health record. EHR typically contains extremely private and important patient information that is routinely disseminated among doctors, radiologists, nurses, chemists, and researchers to aid in accurate diagnosis and treatment. With the use of key exchange protocols, two or more parties can create a shared encryption key that they can use to encrypt or sign data they want to transmit. The expansion to a bigger system may be challenging since key exchange methods with certificates need a reliable third party to confirm the validity of the received messages. As the number of users grows, they require more storage space for certificates and bandwidth for signature verification. Each client and server must be pre-provisioned with a distinct asymmetric Elliptic Curve Cryptography (ECC) in order for the authentication mechanism to work.

**1. INTRODUCTION**

**1.1 INRODUCTION**

The motivation behind this project stems from the growing need for secure and efficient communication in the healthcare sector, particularly during Electronic Health Record (EHR) sharing. With the increasing digitization of medical data, ensuring confidentiality and authentication has become a critical concern. Traditional encryption methods, such as RSA, demand significant computational resources and larger key sizes, making them less practical for real-time applications. The Elliptic Curve-Diffie Hellman (ECC) algorithm offers a more efficient alternative, providing robust security with smaller key sizes, reduced computational overhead, and lower bandwidth consumption. By integrating the Authenticated Key Agreement (AKA) protocol, this project ensures that only authorized users such as doctors and patient can securely establish and exchange session keys over insecure networks. Since these parties do not share a common secret key, the involvement of a control unit for identity verification and secure key exchange becomes essential. This project is driven by the need to enhance the security and integrity of sensitive medical data while enabling seamless and confidential communication between healthcare professionals. By implementing a secure authentication and key exchange mechanism, the system not only strengthens data protection but also fosters trust and compliance with privacy regulations, ultimately improving the efficiency and security of healthcare information management.

**1.2 EXISTING SYSTEM**

In existing system handled manually-largely paper based and lacks standards. All the information need to be recorded in paper which is very a very tedious and time taking task that cannot be implemented in big hospitals. Personal information may also bring privacy leakage problems. Sensitive information can be leaked because of dishonest patients. It is difficult to protect multimedia big data.

**1.2.1 DISADVANTAGES**

* Risk of mismanagement of data.
* Less Security.
* No proper coordination between different Applications and patients.
* Fewer patients - Friendly.
* Accuracy not guaranteed.
* Not in reach of distant patients.

**1.3 PROPOSED SYSTEM**

The first step in setting up a secure communication between two parties is to establish a key. Key Establishment (KE) is a protocol that allows two communicating parties to share a secret key. Proposed scheme can provide ECC based authenticated access and keep communicating information confidential based on physiological features. Implement relatively efficient key exchange and secure session protocols that provide the full guarantee of secure communication. This property ensures that the compromise of the long term private keys of one or more entities does not lead to the compromise of previously agreed session keys established by honest entities in the presence of a passive adversary. When patient need to access data after the session time, they should send request message to the data provider. Data provider itself can accept the request and share the new session key to the data patient.

**1.3.1 ADVANTAGE**

* The proposed work is to identify the properties and parameters that affect the performance of the key agreement and key generation schemes.
* Reduce the data loss.
* Overcome the problems of existing authentication scheme and improve the performance using ECDH and Control Unit.
* High level of security

**2. PROBLEM STATEMENT**

The Elliptic Curve-Diffie Hellman (ECC) is one of the most efficient algorithms for securing data. The ECC is more efficient than other traditional techniques such as Rivest-Shamir-Adleman (RSA) in terms of key size, computation and network bandwidth. The Authenticated Key Agreement (AKA) protocol is used for establishing a common session key between the two communicating parties. Authenticated key agreements enable users to determine session keys, and to securely communicate with others over an insecure channel via the session keys. This proposed work investigates the lower bounds on communications for two-party authenticated key agreements and considers whether or not the sub-keys for generating a session key can be revealed in the channel. Since two clients do not share any common secret key, they require the help of the control unit to authenticate their identities and exchange confidential and authenticated information over insecure networks. However, if the session key security is based on asymmetric cryptosystems, then revealing the sub-keys cannot compromise the session key. Objective of this project is to establish secure communication between doctor and administrator during EHR sharing. An authentication and key exchange scheme is essential to provide confidential communication and mutual authentication between the doctor and the private key generator through an intermediate server. The identification of doctors is carried out through a control unit using key verification process.

**3. LOGICAL DEVELOPMENT**

**3.1 ARCHITECTURE DESIGN**

A system architecture or systems architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. System architecture can comprise system components, the externally visible properties of those components, the relationships (e.g. the behavior) between them. It can provide a plan from which products can be procured, and systems developed, that will work together to implement the overall system. There have been efforts to formalize languages to describe system architecture; collectively these are called architecture description languages (ADLs).

**Various organizations define systems architecture in different ways, including:**

* An allocated arrangement of physical elements which provides the design solution for a consumer product or life-cycle process intended to satisfy the requirements of the functional architecture and the requirements baseline.
* Architecture comprises the most important, pervasive, top-level, strategic inventions, decisions, and their associated rationales about the overall structure (i.e., essential elements and their relationships) and associated characteristics and behavior.
* If documented, it may include information such as a detailed inventory of current hardware, software and networking capabilities; a description of long-range plans and priorities for future purchases, and a plan for upgrading and/or replacing dated equipment and software
* The composite of the design architectures for products and their life-cycle processes.



**Patient**

**Doctor**

**Upload Files**

**Data retrieval**

**Session Checking**

**Receive file information**

**Encryption using ECC algorithm**

**Storage database**

**Decrypt the files**

**Send request**

**View Files list**

**Login**

**Accept / Reject request**

**3.2 DATAFLOW DIAGRAMS**

A two-dimensional diagram explains how data is processed and transferred in a system. The graphical depiction identifies each source of data and how it interacts with other data sources to reach a common output. Individuals seeking to draft a data flow diagram must identify external inputs and outputs, determine how the inputs and outputs relate to each other, and explain with graphics how these connections relate and what they result in. This type of diagram helps business development and design teams visualize how data is processed and identify or improve certain aspects.

**Data flow Symbols:**

| **Symbol** | **Description** |
| --- | --- |
| http://cpanel.stpaulsscience.org/gceict/specifications/ocr/unit3/sdlc/dfd/entity.jpg | An **entity**. A source of data or a destination for data. |
| http://cpanel.stpaulsscience.org/gceict/specifications/ocr/unit3/sdlc/dfd/process.jpg | A **process** or task that is performed by the system. |
| http://cpanel.stpaulsscience.org/gceict/specifications/ocr/unit3/sdlc/dfd/store.jpg | A **data store**, a place where data is held between processes. |
| http://cpanel.stpaulsscience.org/gceict/specifications/ocr/unit3/sdlc/dfd/flow.jpg | A **data flow**. |

**LEVEL 0**

The Level 0 DFD shows how the system is divided into 'sub-systems' (processes), each of which deals with one or more of the data flows to or from an external agent, and which together provide all of the functionality of the system as a whole. It also identifies internal data stores that must be present in order for the system to do its job, and shows the flow of data between the various parts of the system.

Doctor

Database

Patient

**LEVEL-1**

The next stage is to create the Level 1 Data Flow Diagram. This highlights the main functions carried out by the system. As a rule, to describe the system was using between two and seven functions - two being a simple system and seven being a complicated system. This enables us to keep the model manageable on screen or paper.

Patient

Database

**LEVEL-2**

A Data Flow Diagram (DFD) tracks processes and their data paths within the business or system boundary under investigation. A DFD defines each domain boundary and illustrates the logical movement and transformation of data within the defined boundary. The diagram shows 'what' input data enters the domain, 'what' logical processes the domain applies to that data, and 'what' output data leaves the domain. Essentially, a DFD is a tool for process modeling and one of the oldest.

Application Server

Database

**LEVEL-3**

A data flow diagram (DFD) is a graphical representation of the flow of data through an information system. A DFD shows the flow of data from data sources and data stores to processes, and from processes to data stores and data sinks. DFDs are used for modelling and analyzing the flow of data in data processing systems, and are usually accompanied by a data dictionary, an entity-relationship model, and a number of process descriptions.

Doctor

Database

**LEVEL 4**

A DFD may look similar to a flow chart. However, there is a significant difference with the data flow diagram. The arrows in DFDs show that there is a flow of data between the two components and not that the component is sending the data that must be executed in the following component. A component in DFD may not continue execution when sending data and during execution of the component receiving the data. The component sending data can send multiple sets of data along several connections. In fact, a DFD node can be a component that never ends.

Patient

Database

**4. DATABASE DESIGN**

**4.1 TABLE DESIGN**

A table is a data structure that organizes information into rows and columns. It can be used to both store and display data in a structured format. For example, databases store data in tables so that information can be quickly accessed from specific rows. Websites often use tables to display multiple rows of data on page. Spreadsheets combine both purposes of a table by storing and displaying data in a structured format.

Databases often contain multiple tables, with each one designed for a specific purpose. For example, a company database may contain separate tables for employees, clients, and suppliers. Each table may include its own set of fields, based on what data the table needs to store. In database tables, each field is considered a column, while each entry (or record), is considered a row. A specific value can be accessed from the table by requesting data from an individual column and row.

**Table structure for table files**

| **Field** | **Type** | **Null** | **Default** |
| --- | --- | --- | --- |
| ***id*** | int(30) | Yes | NULL |
| oid | varchar(30) | Yes | NULL |
| oname | varchar(30) | Yes | NULL |
| fc | varchar(30) | Yes | NULL |
| bp | varchar(30) | Yes | NULL |
| sugar | varchar(30) | Yes | NULL |
| ran | varchar(100) | Yes | NULL |
| type | varchar(100) | Yes | NULL |
| size | varchar(100) | Yes | NULL |
| file | varchar(100) | Yes | NULL |
| date | varchar(30) | Yes | NULL |
| pub | varchar(30) | Yes | NULL |
| pri | varchar(30) | Yes | NULL |
| status | varchar(30) | Yes | NULL |

**Table structure for table owner**

| **Field** | **Type** | **Null** | **Default** |
| --- | --- | --- | --- |
| ***id*** | int(30) | Yes | NULL |
| name | varchar(30) | Yes | NULL |
| gender | varchar(30) | Yes | NULL |
| mobile | varchar(30) | Yes | NULL |
| gmail | varchar(30) | Yes | NULL |
| address | varchar(100) | Yes | NULL |
| uname | varchar(30) | Yes | NULL |
| pass | varchar(30) | Yes | NULL |
| cpass | varchar(30) | Yes | NULL |
| ran | varchar(30) | Yes | NULL |
| pri | varchar(30) | Yes | NULL |
| pub | varchar(30) | Yes | NULL |
| status | varchar(30) | Yes | NULL |
| report | varchar(30) | Yes | NULL |
| cd | varchar(30) | Yes | NULL |

**Table structure for table request**

| **Field** | **Type** | **Null** | **Default** |
| --- | --- | --- | --- |
| ***id*** | int(30) | Yes | NULL |
| uid | varchar(30) | Yes | NULL |
| uname | varchar(30) | Yes | NULL |
| oid | varchar(30) | Yes | NULL |
| oname | varchar(30) | Yes | NULL |
| fc | varchar(30) | Yes | NULL |
| file | varchar(30) | Yes | NULL |
| ran | varchar(30) | Yes | NULL |
| pri | varchar(30) | Yes | NULL |
| status | varchar(30) | Yes | NULL |
| report | varchar(30) | Yes | NULL |
| sta | varchar(30) | Yes | NULL |
| date | varchar(30) | Yes | NULL |
| time | varchar(30) | Yes | NULL |
| mail | varchar(30) | Yes | NULL |

**Table structure for table user**

| **Field** | **Type** | **Null** | **Default** |
| --- | --- | --- | --- |
| ***id*** | int(30) | Yes | NULL |
| name | varchar(30) | Yes | NULL |
| gender | varchar(30) | Yes | NULL |
| mobile | varchar(30) | Yes | NULL |
| gmail | varchar(30) | Yes | NULL |
| address | varchar(100) | Yes | NULL |
| uname | varchar(30) | Yes | NULL |
| pass | varchar(30) | Yes | NULL |
| cpass | varchar(30) | Yes | NULL |
| ran | varchar(30) | Yes | NULL |
| status | varchar(30) | Yes | NULL |
| report | varchar(30) | Yes | NULL |
| cd | varchar(30) | Yes | NULL |

**4.2 RELTIONSHIP DIAGRAM**

**files**

**request**

Update

**owner**

**user**

**5. PROGRAM DESIGN**

**5.1 MODULES DESCRIPTION**

* Authentication Framework
* User Enrolment
* Key Distribution
* EHR Sharing
* Key and Session Verification

**MODULE DESCRIPTION**

**5.1.1 AUTHENTICATION FRAMEWORK**

Admin should create secure EHR sharing framework.The security of the communication between doctors and patient the intermediate server is based on a Session based Authentication and a Key Exchange (AKE) scheme that provides mutual authentication between doctors and the doctor through a control unit. Thencreate control unit that used for verification process.Set security parameters and key generation functions.

**5.1.2 USER ENROLMENT**

User enrolment is the process of registering with application to make communications. Here users are defined as doctor and patient. Both are registered in this application and get authentication keys for login process. For registering process, they should enter the details like name, father name, gender, age, mobile number, email id, username and password. Registered details are sending to the control unit for confirmation.

**5.1.3 KEY DISTRIBUTION**

Key distribution is the process of generating secret keys and distributing the keys to the registered patients. Control unit take responsible for key generation and distribution process. In proposed work, ECDH based key generation scheme has been implemented. Then the keys will be sharing to the registered patients through their mail id. The Elliptic Curve-Diffie Hellman (ECDH) is one of the most efficient algorithms for securing data. The ECDH is more efficient than other traditional techniques such as Rivest-Shamir-Adleman (RSA) in terms of key size, computation and network bandwidth. The Authenticated Key Agreement (AKA) protocol is used for establishing a common session key between the two communicating parties. Authenticated key agreements enable patients to determine session keys, and to securely communicate with others over an insecure channel via the session keys.

**5.1.4 EHR SHARING**

This module explains about EHR sharing by patient. Doctor should authenticated by control unit using username, password and secret key. The entered details are validated by control unit. Then they will be allowed to share medical information to the patients. . This proposed work investigates the lower bounds on communications for two-party authenticated key agreements and considers whether or not the sub-keys for generating a session key can be revealed in the channel. Since two clients do not share any common secret key, they require the help of the control unit to authenticate their identities and exchange confidential and authenticated information over insecure networks. However, if the session key security is based on asymmetric cryptosystems, then revealing the sub-keys cannot compromise the session key.

**5.1.5 KEY AND SESSION VERIFICATION**

In this module data access process has been explained. Data access is the process of accessing shared EHR by doctor. Before accessing EHR, Doctors should authenticated using their username, password and login key. After that doctors session time will be checking by the system. When all details entered by the doctors are correct including the session time, then they will be allowing accessing EHR from proposed framework. If the session time gets lost, they will be send request to the doctor to share new key permission.

**5.2 NETWORK SECURITY DEFINITION**

**NETWORK SECURITY**

Network Security is a branch of cybersecurity focused on protecting computer networks and data from unauthorized access, misuse, or theft. It encompasses a set of rules, policies, and technologies designed to safeguard the integrity, confidentiality, and availability of information as it travels across or is stored within a network. The primary goal of network security is to create a secure platform for users, applications, and devices to communicate without interference from malicious actors. Network Security includes a wide range of components and practices, such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), virtual private networks (VPNs), encryption, antivirus software, and access control mechanisms. It also involves constant monitoring, network segmentation, vulnerability assessments, and the application of security patches to prevent potential exploits. Both hardware and software tools are used to implement these security measures in enterprise and personal networks. A common example of network security in action is the use of a firewall in a corporate environment. Firewalls are deployed to monitor incoming and outgoing traffic and block malicious activity based on a predefined set of rules. For instance, a company might configure a firewall to restrict access to its internal server network from external IP addresses, ensuring that only authorized personnel can access sensitive business data remotely through a secured VPN tunnel. The advantages of network security are numerous. It protects sensitive data from breaches and cyberattacks, helps maintain the trust of customers and clients, and ensures the continuity of business operations by preventing disruptions caused by malware or hacking attempts. Additionally, robust network security reduces financial losses associated with data theft and system downtimes, and it also helps organizations comply with legal and regulatory requirements regarding data privacy and security.

**5.3 ALGORITHM**

**Elliptical Curve Cryptography**

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. Elliptic curves are an algebraic structure and their use for cryptography. They feature properties which allow the setup of a problem similar to the well-known discrete logarithm problem of finite fields – also known as Galois fields (GF).ECC includes key agreement, encryption, and digital signature algorithms. The key distribution algorithm is used to share a secret key, the encryption algorithm enables confidential communication, and the digital signature algorithm is used to authenticate the signer and validate the integrity of the message:

**ECC ALGORITHM STEPS**

Assume that those who are going through this article will have a basic understanding of cryptography (terms like encryption and decryption).

The equation of an elliptic curve is given as,

Description: https://bithin.files.wordpress.com/2012/02/eccequation.png?w=500

Few terms that will be used,

**E -> Elliptic Curve**

**P -> Point on the curve**

**n -> Maximum limit ( This should be a prime number )**

**Key Generation**

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver’s public key and the receiver will decrypt its private key.

Now, we have to select a number **‘d’**within the range of **‘n’**.

Using the following equation we can generate the public key

Q = d \* P

**d** = The random number that we have selected within the range of (**1 to n-1**). **P** is the point on the curve.

**‘Q’ is the public key** and ‘d’ **is the private key.**

**Encryption**

Let ‘m’ be the message that we are sending. We have to represent this message on the curve. This has in-depth implementation details. All the advance research on ECC is done by a company called certicom.

Consider *‘m’* has the point *‘M’* on the curve *‘E’.* Randomly select ‘k’ from [1 – (n-1)].

Two cipher texts will be generated let it be **C1** and **C2**.

**C1 = k\*P, C2 = M + k\*Q.**C1 and C2 will be send.

Decryption

We have to get back the message ‘m’ that was send to us,

**M = C2 – d \* C1**

M is the original message that we have send.

Proof

How do we get back the message?

M = C2 – d \* C1

‘M’ can be represented as ‘C2 – d \* C1’

C2 – d \* C1 = (M + k \* Q) – d \* (k \* P )          ( C2 = M + k \* Q and C1 = k \* P )

= M + k \* d \* P – d \* k \*P          (canceling out k \* d \* P)

= M (Original Message)

**6. TESTING**

Testing is a set activity that can be planned and conducted systematically. Testing begins at the module level and work towards the integration of entire computers based system. Nothing is complete without testing, as it is vital success of the system.

Testing Objectives:

There are several rules that can serve as testing objectives, they are

1. Testing is a process of executing a program with the intent of finding an error
2. A good test case is one that has high probability of finding an undiscovered error.
3. A successful test is one that uncovers an undiscovered error.

If testing is conducted successfully according to the objectives as stated above, it would uncover errors in the software. Also testing demonstrates that software functions appear to the working according to the specification, that performance requirements appear to have been met.

There are three ways to test a program

1. For Correctness
2. For Implementation efficiency
3. For Computational Complexity.

Tests used for implementation efficiency attempt to find ways to make a correct program faster or use less storage. It is a code-refining process, which reexamines the implementation phase of algorithm development. Tests for computational complexity amount to an experimental analysis of the complexity of an algorithm or an experimental comparison of two or more algorithms, which solve the same problem.

The data is entered in all forms separately and whenever an error occurred, it is corrected immediately. A quality team deputed by the management verified all the necessary documents and tested the Software while entering the data at all levels.

**6.1 TYPES OF TESTING**

The development process involves various types of testing. Each test type addresses a specific testing requirement. The most common types of testing involved in the development process are:

* Unit Test
* Functional Test
* Integration Test
* System Test
* Validation Test

**Unit Testing:**

The first test in the development process is the unit test. The source code is normally divided into modules, which in turn are divided into smaller units called units. These units have specific behavior. The test done on these units of code is called unit test. Unit test depends upon the language on which the project is developed. Unit tests ensure that each unique path of the project performs accurately to the documented specifications and contains clearly defined inputs and expected results.

**Functional Testing:**

Functional test can be defined as testing two or more modules together with the intent of finding defects, demonstrating that defects are not present, verifying that the module performs its intended functions as stated in the specification and establishing confidence that a program does what it is supposed to do.

**Integration Testing:**

In integration testing modules are combined and tested as a group. Modules are typically code modules, individual applications, source and destination applications on a network, etc. Integration Testing follows unit testing and precedes system testing. Testing after the product is code complete. Betas are often widely distributed or even distributed to the public at large in hopes that they will buy the final product when it is released.

**System Testing**

System testing is defined as testing of a complete and fully integrated software product. This testing falls in black-box testing wherein knowledge of the inner design of the code is not a pre-requisite and is done by the testing team. It is the final test to verify that the product to be delivered meets the specifications mentioned in the requirement document. It should investigate both functional and non-functional requirements.

**Validation Testing**

The process of evaluating software during the development process or at the end of the development process to determine whether it satisfies specified business requirements. Validation Testing ensures that the product actually meets the client's needs. It can also be defined as to demonstrate that the product fulfills its intended use when deployed on appropriate environment.

**6.2 TEST REPORT**

**Test Case Design**

| **Test case ID** | **Test Plan ID** | **Test case** | **Actual Input** | **Actual Output** | **Expected Output** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| TC01 | TC01 | User Registration | User Personal details | Register page Design | Register page design | Pass |

1. **Plan of Action**

* **Requirement analysis Plan**

1. Execution qualities, such as safety, security and usability, which are observable during operation (at run time).
2. Evolution qualities, such as [testability](https://en.wikipedia.org/wiki/Software_testability), maintainability, extensibility and scalability, which are embodied in the static structure of the system.

* **Development of Modules**
* Authentication Framework
* User Enrolment
* Key Distribution
* EHR Sharing
* Key and Session Verification
* **Test Case Plan**

Testing Level Specific Test Plans**:** Plans for each level of testing.

* Unit Test Plan
* Integration Test Plan
* System Test Plan
* Acceptance Test Plan

**7. CONCLUSION**

In conclusion, implementing secure data sharing using the Elliptic Curve Cryptography (ECC) algorithm offers a robust solution with significant advantages. ECC provides a high level of security while maintaining efficiency, making it suitable for applications where both security and performance are crucial. Our design ensures that files are encrypted using the recipient's public key, guaranteeing that only the intended recipient can decrypt the data using their private key. By employing ECC, we can protect sensitive information during transfer, mitigating the risk of unauthorized access. Additionally, our approach includes measures to secure key management and considers potential vulnerabilities, ensuring a comprehensive security strategy. Overall, ECC is a reliable choice for secure data sharing, offering a balance between security, efficiency, and practicality

**7.1 FUTURE ENHANCEMENTS**

In future, implement more advanced key management techniques, such as key rotation and key revocation, to enhance the security of the system

**8. REFERENCES**

[1] Vengala, Dilip Venkata Kumar, D. Kavitha, and AP Siva Kumar. "Three factor authentication system with modified ECC based secured data transfer: untrusted cloud environment." Complex & Intelligent Systems 9.3 (2023): 2915-2928.

[2] Huang, Wenfeng. "ECC-based three-factor authentication and key agreement scheme for wireless sensor networks." *Scientific Reports* 14.1 (2024): 1787.

[3] Mahajan, Hemant B., and Aparna A. Junnarkar. "Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing." *Multimedia Tools and Applications* 82.28 (2023): 44335-44358.

[4] Chandrika, S. Udhaya, and T. Pramananda Perumal. "Modified ECC for Secure data transfer in multi-tenant cloud computing." *International Journal of Computer Network and Information Security* 9.6 (2022): 76.

[5] Sammy, F., and S. Maria Celestin Vigila. "An Efficient Blockchain Based Data Access with Modified Hierarchical Attribute Access S

[6] Hu, Shunfang, et al. "Provably secure ECC-based anonymous authentication and key Agreement for IoT." *Applied Sciences* 14.8 (2024): 3187.

[7] Zhang, Duo, et al. "A Secure and Privacy‐Preserving Medical Data Sharing via Consortium Blockchain." *Security and Communication Networks* 2022.1 (2022): 2759787.

[8] Ryu, Jongseok, et al. "Secure ECC-based three-factor mutual authentication protocol for telecare medical information system." *IEEE Access* 10 (2022): 11511-11526.

[9] Yao, Hailong, et al. "ECC-based lightweight authentication and access control scheme for IoT E-healthcare." *Soft Computing* 26.9 (2022): 4441-4461.

[10] Narayanan, Uma, Varghese Paul, and Shelbi Joseph. "A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment." *Journal of King Saud University-Computer and Information Sciences* 34.6 (2022): 3121-3135.

**9. APPENDIX**

**9.1 SOURCE CODE**

Admin.jsp :

<%

try

{

String btn=request.getParameter("Submit");

if(btn.equals("Submit"))

{

String name=request.getParameter("name");

String pass=request.getParameter("pass");

if((name.equals("admin")) && (pass.equals("admin")))

{

%>

<script language="javascript">

alert("Login Successful");

window.location.href="admin\_home.jsp";

</script>

<%

}

else

{

%>

<script language="javascript">

alert("Login Failed");

window.location.href="admin.jsp";

</script>

<%

}

}

}

catch(Exception e)

{

}

%>

<html>

<head>

<title>ECC Data Sharing</title>

<meta charset="utf-8">

<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">

<link href="layout/styles/layout.css" rel="stylesheet" type="text/css" media="all">

<style type="text/css">

<!--

table, tr, td {

border: 3px white;

}

tr.noBorder td {

border: 0;

}

.style2 {

color: #FF00FF;

font-style: italic;

font-weight: bold;

}

.style3 {color: #993333}

.style6 {color: #000000}

-->

</style>

</head>

<body id="top">

<div class="wrapper row0">

<div id="topbar" class="hoc clear">

<div class="fl\_left">

<ul class="nospace inline pushright">

<li><i class="fa fa-phone"></i> +00 (123) 456 7890</li>

<li><i class="fa fa-envelope-o"></i> info@domain.com</li>

</ul>

</div>

<div class="fl\_right">

<ul class="nospace inline pushright">

<li><i class="fa fa-sign-in"></i> <a href="#">Login</a></li>

<li><i class="fa fa-user"></i> <a href="#">Register</a></li>

</ul>

</div>

</div>

</div>

<div class="wrapper row1">

<header id="header" class="hoc clear">

<div id="logo" class="fl\_left">

<h1><a href="index.jsp">Ecc Data Sharing</a></h1>

</div>

<div id="search" class="fl\_right">

<form class="clear" method="post" action="#">

<fieldset>

<legend>Search:</legend>

<input type="search" value="" placeholder="Search Here&hellip;">

<button class="fa fa-search" type="submit" title="Search"><em>Search</em></button>

</fieldset>

</form>

</div>

</header>

</div>

<div class="wrapper row2">

<nav id="mainav" class="hoc clear">

<ul class="clear">

<li ><a href="index.jsp">Home</a></li>

<li class="active"><a href="admin.jsp">Admin</a></li>

<li><a href="owner.jsp">Data Owner</a></li>

<li><a href="user.jsp">Data User</a></li>

</ul>

</nav>

</div>

<div class="wrapper bgded" style="background-image:url('images/demo/backgrounds/ecc.png');">

<div id="pageintro" class="hoc clear">

<article>

<div class="overlay inspace-30 btmspace-30">

<h2 class="heading">Ecc Data Sharing</h2>

<p>Electronic health records possess the patient&#39;s medication details and their health history.</p>

</div>

</article>

</div>

</div>

<form id="form" name="form" method="post" action="">

<table width="200">

<tr>

<td width="39%" height="48">&nbsp;</td>

<td colspan="2"><div align="center" class="style1 style3">Admin Login : </div></td>

<td width="30%">&nbsp;</td>

</tr>

<tr>

<td height="49">&nbsp;</td>

<td width="11%"><div align="center" class="style6">Name : </div></td>

<td width="20%"><input name="name" type="text" class="style6"></td>

<td>&nbsp;</td>

</tr>

<tr>

<td height="49">&nbsp;</td>

<td><div align="center" class="style6">Password : </div></td>

<td><input name="pass" type="password" class="style6"></td>

<td>&nbsp;</td>

</tr>

<tr>

<td height="47">&nbsp;</td>

<td><div align="center">

<input name="Submit" type="submit" class="row1" value="Submit">

</div></td>

<td><input name="Clear" type="reset" class="row1" value="Clear"></td>

<td>&nbsp;</td>

</tr>

</table>

</form>

<div class="wrapper row4 bgded overlay" style="background-image:url('images/demo/backgrounds/ecc1.jpg');">

<footer id="footer" class="hoc clear">

<div id="cta" class="group">

<div class="one\_third first"><i class="fa fa-map-marker"></i>

<p>Find us</p>

<p><a href="#">Google Maps</a></p>

</div>

<div class="one\_third"><i class="fa fa-phone"></i>

<p>Call us</p>

<p>+00 (123) 456 7890</p>

</div>

<div class="one\_third"><i class="fa fa-envelope-o"></i>

<p>Email us</p>

<p>info@domain.com</p>

</div>

</div>

<div class="group">

<div class="one\_quarter first">

<h6 class="title">ECC Data Sharing</h6>

<p>EHR generally

contains highly-sensitive and critical data related to patients, which is frequently shared

among clinicians, radiologists, healthcare providers, pharmacists, and researchers, for

effective diagnosis and treatment.</p>

</div>

<div class="one\_quarter">

<h6 class="title">Level 0</h6>

<ul class="nospace linklist">

<li><a href="#">Authentication Framework</a></li>

<li><a href="#">User Enrollment</a></li>

<li><a href="#">Key Destribution</a></li>

<li><a href="#">EHR sharing</a></li>

<li><a href="#">Key and Session Verification</a></li>

</ul>

</div>

<div class="one\_quarter">

<h6 class="title">Level 1</h6>

<ul class="nospace linklist">

<li><a href="#">Security</a></li>

<li><a href="#">Encryption</a></li>

<li><a href="#">Decryption</a></li>

<li><a href="#">Data Hiding</a></li>

<li><a href="#">Data Sharing</a></li>

</ul>

</div>

<div class="one\_quarter">

<h6 class="title">Techniques</h6>

<ul class="nospace linklist">

<li>

<article>

<p class="nospace">Key exchange protocols enable two or more parties to

establish a shared encryption key that they can use to encrypt</p>

</article>

</li>

<li>

<article>

<p class="nospace">sign data that they plan to

exchange. As key exchange schemes with certificates require some trusted authority</p>

</article>

</li>

</ul>

</div>

</div>

</footer>

</div>

<div class="wrapper row5">

<div id="social" class="hoc clear">

<div class="one\_half first">

<h6 class="title">Social Media</h6>

<ul class="faico clear">

<li><a class="faicon-facebook" href="#"><i class="fa fa-facebook"></i></a></li>

<li><a class="faicon-pinterest" href="#"><i class="fa fa-pinterest"></i></a></li>

<li><a class="faicon-twitter" href="#"><i class="fa fa-twitter"></i></a></li>

<li><a class="faicon-dribble" href="#"><i class="fa fa-dribbble"></i></a></li>

<li><a class="faicon-linkedin" href="#"><i class="fa fa-linkedin"></i></a></li>

<li><a class="faicon-google-plus" href="#"><i class="fa fa-google-plus"></i></a></li>

<li><a class="faicon-vk" href="#"><i class="fa fa-vk"></i></a></li>

<li><a class="faicon-youtube" href="#"><i class="fa fa-youtube"></i></a></li>

<li><a class="faicon-rss" href="#"><i class="fa fa-rss"></i></a></li>

</ul>

</div>

<div class="one\_half">

<h6 class="title">Join our community :</h6>

<form class="clear" method="post" action="#">

<fieldset>

<legend>Newsletter:</legend>

<input type="text" value="" placeholder="Type Email Here&hellip;">

<button class="fa fa-share" type="submit" title="Submit"><em>Submit</em></button>

</fieldset>

</form>

</div>

</div>

</div>

<div class="wrapper row6">

<div id="copyright" class="hoc clear">

<p class="fl\_left"> <a href="#"></a></p>

<p class="fl\_right"> <a target="\_blank" href="http://www.os-templates.com/" title="Free Website Templates"></a></p>

</div>

</div>

<a id="backtotop" href="#top"><i class="fa fa-chevron-up"></i></a>

<!-- JAVASCRIPTS -->

<script src="layout/scripts/jquery.min.js"></script>

<script src="layout/scripts/jquery.backtotop.js"></script>

<script src="layout/scripts/jquery.mobilemenu.js"></script>

<!-- IE9 Placeholder Support -->

<script src="layout/scripts/jquery.placeholder.min.js"></script>

<!-- / IE9 Placeholder Support -->

</body>

</html>

Admin Home.jsp

<html>

<head>

<title>ECC Data Sharing</title>

<meta charset="utf-8">

<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">

<link href="layout/styles/layout.css" rel="stylesheet" type="text/css" media="all">

<style type="text/css">

<!--

table, tr, td {

border: 3px white;

}

tr.noBorder td {

border: 0;

}

.style2 {

color: #FF00FF;

font-style: italic;

font-weight: bold;

}

.style3 {color: #993333}

.style6 {color: #000000}

-->

</style>

</head>

<body id="top">

<div class="wrapper row0">

<div id="topbar" class="hoc clear">

<div class="fl\_left">

<ul class="nospace inline pushright">

<li><i class="fa fa-phone"></i> +00 (123) 456 7890</li>

<li><i class="fa fa-envelope-o"></i> info@domain.com</li>

</ul>

</div>

<div class="fl\_right">

<ul class="nospace inline pushright">

<li><i class="fa fa-sign-in"></i> <a href="#">Login</a></li>

<li><i class="fa fa-user"></i> <a href="#">Register</a></li>

</ul>

</div>

</div>

</div>

<div class="wrapper row1">

<header id="header" class="hoc clear">

<div id="logo" class="fl\_left">

<h1><a href="index.jsp">Ecc Data Sharing</a></h1>

</div>

<div id="search" class="fl\_right">

<form class="clear" method="post" action="#">

<fieldset>

<legend>Search:</legend>

<input type="search" value="" placeholder="Search Here&hellip;">

<button class="fa fa-search" type="submit" title="Search"><em>Search</em></button>

</fieldset>

</form>

</div>

</header>

</div>

<div class="wrapper row2">

<nav id="mainav" class="hoc clear">

<ul class="clear">

<li class="active"><a href="admin\_home.jsp">Home</a></li>

<li><a href="admin\_ownerapprove.jsp">Owner Approve</a></li>

<li><a href="admin\_userapprove.jsp">User Approve</a></li>

<li><a href="index.jsp">Logout </a></li>

</ul>

</nav>

</div>

<div class="wrapper bgded" style="background-image:url('images/demo/backgrounds/ecc.png');">

<div id="pageintro" class="hoc clear">

<article>

<div class="overlay inspace-30 btmspace-30">

<h2 class="heading">Ecc Data Sharing</h2>

<p>Electronic health records possess the patient&#39;s medication details and their health history.</p>

</div>

</article>

</div>

</div>

<div class="wrapper row4 bgded overlay" style="background-image:url('images/demo/backgrounds/ecc1.jpg');">

<footer id="footer" class="hoc clear">

<div id="cta" class="group">

<div class="one\_third first"><i class="fa fa-map-marker"></i>

<p>Find us</p>

<p><a href="#">Google Maps</a></p>

</div>

<div class="one\_third"><i class="fa fa-phone"></i>

<p>Call us</p>

<p>+00 (123) 456 7890</p>

</div>

<div class="one\_third"><i class="fa fa-envelope-o"></i>

<p>Email us</p>

<p>info@domain.com</p>

</div>

</div>

<div class="group">

<div class="one\_quarter first">

<h6 class="title">ECC Data Sharing</h6>

<p>EHR generally

contains highly-sensitive and critical data related to patients, which is frequently shared

among clinicians, radiologists, healthcare providers, pharmacists, and researchers, for

effective diagnosis and treatment.</p>

</div>

<div class="one\_quarter">

<h6 class="title">Level 0</h6>

<ul class="nospace linklist">

<li><a href="#">Authentication Framework</a></li>

<li><a href="#">User Enrollment</a></li>

<li><a href="#">Key Destribution</a></li>

<li><a href="#">EHR sharing</a></li>

<li><a href="#">Key and Session Verification</a></li>

</ul>

</div>

<div class="one\_quarter">

<h6 class="title">Level 1</h6>

<ul class="nospace linklist">

<li><a href="#">Security</a></li>

<li><a href="#">Encryption</a></li>

<li><a href="#">Decryption</a></li>

<li><a href="#">Data Hiding</a></li>

<li><a href="#">Data Sharing</a></li>

</ul>

</div>

<div class="one\_quarter">

<h6 class="title">Techniques</h6>

<ul class="nospace linklist">

<li>

<article>

<p class="nospace">Key exchange protocols enable two or more parties to

establish a shared encryption key that they can use to encrypt</p>

</article>

</li>

<li>

<article>

<p class="nospace">sign data that they plan to

exchange. As key exchange schemes with certificates require some trusted authority</p>

</article>

</li>

</ul>

</div>

</div>

</footer>

</div>

<div class="wrapper row5">

<div id="social" class="hoc clear">

<div class="one\_half first">

<h6 class="title">Social Media</h6>

<ul class="faico clear">

<li><a class="faicon-facebook" href="#"><i class="fa fa-facebook"></i></a></li>

<li><a class="faicon-pinterest" href="#"><i class="fa fa-pinterest"></i></a></li>

<li><a class="faicon-twitter" href="#"><i class="fa fa-twitter"></i></a></li>

<li><a class="faicon-dribble" href="#"><i class="fa fa-dribbble"></i></a></li>

<li><a class="faicon-linkedin" href="#"><i class="fa fa-linkedin"></i></a></li>

<li><a class="faicon-google-plus" href="#"><i class="fa fa-google-plus"></i></a></li>

<li><a class="faicon-vk" href="#"><i class="fa fa-vk"></i></a></li>

<li><a class="faicon-youtube" href="#"><i class="fa fa-youtube"></i></a></li>

<li><a class="faicon-rss" href="#"><i class="fa fa-rss"></i></a></li>

</ul>

</div>

<div class="one\_half">

<h6 class="title">Join our community :</h6>

<form class="clear" method="post" action="#">

<fieldset>

<legend>Newsletter:</legend>

<input type="text" value="" placeholder="Type Email Here&hellip;">

<button class="fa fa-share" type="submit" title="Submit"><em>Submit</em></button>

</fieldset>

</form>

</div>

</div>

</div>

<div class="wrapper row6">

<div id="copyright" class="hoc clear">

<p class="fl\_left"> <a href="#"></a></p>

<p class="fl\_right"> <a target="\_blank" href="http://www.os-templates.com/" title="Free Website Templates"></a></p>

</div>

</div>

<a id="backtotop" href="#top"><i class="fa fa-chevron-up"></i></a>

<!-- JAVASCRIPTS -->

<script src="layout/scripts/jquery.min.js"></script>

<script src="layout/scripts/jquery.backtotop.js"></script>

<script src="layout/scripts/jquery.mobilemenu.js"></script>

<!-- IE9 Placeholder Support -->

<script src="layout/scripts/jquery.placeholder.min.js"></script>

<!-- / IE9 Placeholder Support -->

</body>

</html>

Admin owner approve.jsp

<%@ include file="include/dbconnect.jsp" %>

<%@page import="java.util.Random"%>

<%@page import="java.sql.ResultSet"%>

<html>

<head>

<title>ECC Data Sharing</title>

<meta charset="utf-8">

<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">

<link href="layout/styles/layout.css" rel="stylesheet" type="text/css" media="all">

<style type="text/css">

<!--

table, tr, td {

border: 3px white;

}

tr.noBorder td {

border: 0;

}

.style4 {

font-size: 18px;

color: #993333;

}

.style5 {font-size: 18px}

.style6 {color: #000000}

.style7 {font-size: 14px}

-->

</style>

</head>

<body id="top">

<div class="wrapper row0">

<div id="topbar" class="hoc clear">

<div class="fl\_left">

<ul class="nospace inline pushright">

<li><i class="fa fa-phone"></i> +00 (123) 456 7890</li>

<li><i class="fa fa-envelope-o"></i> info@domain.com</li>

</ul>

</div>

<div class="fl\_right">

<ul class="nospace inline pushright">

<li><i class="fa fa-sign-in"></i> <a href="#">Login</a></li>

<li><i class="fa fa-user"></i> <a href="#">Register</a></li>

</ul>

</div>

</div>

</div>

<div class="wrapper row1">

<header id="header" class="hoc clear">

<div id="logo" class="fl\_left">

<h1><a href="index.jsp">Ecc Data Sharing</a></h1>

</div>

<div id="search" class="fl\_right">

<form class="clear" method="post" action="#">

<fieldset>

<legend>Search:</legend>

<input type="search" value="" placeholder="Search Here&hellip;">

<button class="fa fa-search" type="submit" title="Search"><em>Search</em></button>

</fieldset>

</form>

</div>

</header>

</div>

<div class="wrapper row2">

<nav id="mainav" class="hoc clear">

<ul class="clear">

<li><a href="admin\_home.jsp">Home</a></li>

<li class="active"><a href="admin\_ownerapprove.jsp">Owner Approve</a></li>

<li><a href="admin\_userapprove.jsp">User Approve</a></li>

<li><a href="index.jsp">Logout </a></li>

</ul>

</nav>

</div>

<div class="wrapper bgded" style="background-image:url('images/demo/backgrounds/ecc.png');">

<div id="pageintro" class="hoc clear">

<article>

<div class="overlay inspace-30 btmspace-30">

<h2 class="heading">Ecc Data Sharing</h2>

<p>Electronic health records possess the patient&#39;s medication details and their health history.</p>

</div>

</article>

</div>

</div>

<form action="" method="post" name="form1" id="form1" >

<p>&nbsp;</p>

<table width="81%" border="0" align="center">

<%

String uid=(String) session.getAttribute("uid");

ResultSet rs0 = stmt3.executeQuery("select \* from owner where status='0' && report='0' ");

int s = 0;

while (rs0.next()) {

if (s == 0) {

%>

<tr>

<td height="62" colspan="8"><div align="center" class="style4">Owner Request </div></td>

</tr>

<tr>

<td width="51" height="32"><h4 align="center" class="style1"><strong><span class="style7 style1 style5 style6"><em>Id</em></span></strong></h4></td>

<td width="114"><h4 align="center" class="style1 style7 style5 style6"><em><strong>Name</strong></em></h4></td>

<td width="114"><h4 align="center" class="style1 style7 style6 style5"><em><strong>Gender</strong></em></h4></td>

<td width="146"><h4 align="center" class="style1 style7 style5 style6"><em><strong>Mobile</strong></em></h4></td>

<td width="158"><h4 align="center" class="style1 style7 style6 style5"><em><strong>Gmail</strong></em></h4></td>

<td width="158"><h4 align="center" class="style1 style7 style5 style6"><em><strong>Address</strong></em></h4></td>

<td width="158"><h4 align="center" class="style7 style1 style6 style5"><em><strong>Status</strong></em></h4></td>

<td width="158"><h4 align="center" class="style1 style7 style5 style6"><em><strong>Approved</strong></em></h4></td>

</tr>

<%

}

s++;

%>

<tr>

<td height="42"><div align="center"><span class="style6">

<% out.print(s);%>

</span></div></td>

<td><div align="center"><span class="style6">

<% out.print(rs0.getString("name"));%>

</span></div></td>

<td><div align="center"><span class="style6">

<% out.print(rs0.getString("gender"));%>

</span></div></td>

<td><div align="center"><span class="style6">

<% out.print(rs0.getString("mobile"));%>

</span></div></td>

<td><div align="center"><span class="style6">

<% out.print(rs0.getString("gmail"));%>

</span></div></td>

<td><div align="center"><span class="style6">

<% out.print(rs0.getString("address"));%>

</span></div></td>

<td><div align="center"><span class="style6">

<%

String sta=rs0.getString("status");

if(sta.equalsIgnoreCase("0"))

{

out.print("waiting");

}

else

{

out.print("approved");

}

%>

</span></div></td>

<td> <div align="center"><a href="approve\_owner.jsp?fid=<% out.print(rs0.getString("id"));%>"> Approved</a></div></td>

</tr>

<%

}

%>

</table>

<p>&nbsp;</p>

<p>&nbsp;</p>

<p>&nbsp;</p>

</form>

<form action="" method="post" name="form1" id="form1" >

<p>&nbsp;</p>

<table width="81%" border="0" align="center">

<%

ResultSet rs = stmt4.executeQuery("select \* from owner where report!='1' && cd='1' ");

int s1 = 0;

while (rs.next()) {

if (s1 == 0) {

%>

<tr>

<td height="55" colspan="7"><div align="center" class="style4">Approved Owners : </div></td>

</tr>

<tr>

<td width="51" height="32"><h4 align="center" class="style1"><strong><span class="style1 style6 style7"><em>Id</em></span></strong></h4></td>

<td width="114"><h4 align="center" class="style1 style7 style6"><em><strong>Name</strong></em></h4></td>

<td width="114"><h4 align="center" class="style1 style7 style6"><em><strong>Gender</strong></em></h4></td>

<td width="146"><h4 align="center" class="style1 style7 style6"><em><strong>Mobile</strong></em></h4></td>

<td width="158"><h4 align="center" class="style1 style7 style6"><em><strong>Gmail</strong></em></h4></td>

<td width="158"><h4 align="center" class="style1 style7 style6"><em><strong>Address</strong></em></h4></td>

<td width="158"><h4 align="center" class="style7 style1 style6"><em><strong>Status</strong></em></h4></td>

</tr>

<%

}

s1++;

%>

<tr>

<td height="42"><div align="center"><span class="style6">

<% out.print(s1);%>

</span></div></td>

<td><div align="center"><span class="style6">

<% out.print(rs.getString("name"));%>

</span></div></td>

<td><div align="center"><span class="style6">

<% out.print(rs.getString("gender"));%>

</span></div></td>

<td><div align="center"><span class="style6">

<% out.print(rs.getString("mobile"));%>

</span></div></td>

<td><div align="center"><span class="style6">

<% out.print(rs.getString("gmail"));%>

</span></div></td>

<td><div align="center"><span class="style6">

<% out.print(rs.getString("address"));%>

</span></div></td>

<td><div align="center"><span class="style6">

<%

String sta=rs.getString("report");

if(sta.equalsIgnoreCase("0"))

{

out.print("waiting");

}

else

{

out.print("approved");

}

%>

</span></div></td>

</tr>

<%

}

%>

</table>

<p>&nbsp;</p>

<p>&nbsp;</p>

<p>&nbsp;</p>

<p>&nbsp;</p>

<p>&nbsp;</p>

<p>&nbsp;</p>

</form>

<div class="wrapper row4 bgded overlay" style="background-image:url('images/demo/backgrounds/ecc1.jpg');">

<footer id="footer" class="hoc clear">

<div id="cta" class="group">

<div class="one\_third first"><i class="fa fa-map-marker"></i>

<p>Find us</p>

<p><a href="#">Google Maps</a></p>

</div>

<div class="one\_third"><i class="fa fa-phone"></i>

<p>Call us</p>

<p>+00 (123) 456 7890</p>

</div>

<div class="one\_third"><i class="fa fa-envelope-o"></i>

<p>Email us</p>

<p>info@domain.com</p>

</div>

</div>

<div class="group">

<div class="one\_quarter first">

<h6 class="title">ECC Data Sharing</h6>

<p>EHR generally

contains highly-sensitive and critical data related to patients, which is frequently shared

among clinicians, radiologists, healthcare providers, pharmacists, and researchers, for

effective diagnosis and treatment.</p>

</div>

<div class="one\_quarter">

<h6 class="title">Level 0</h6>

<ul class="nospace linklist">

<li><a href="#">Authentication Framework</a></li>

<li><a href="#">User Enrollment</a></li>

<li><a href="#">Key Destribution</a></li>

<li><a href="#">EHR sharing</a></li>

<li><a href="#">Key and Session Verification</a></li>

</ul>

</div>

<div class="one\_quarter">

<h6 class="title">Level 1</h6>

<ul class="nospace linklist">

<li><a href="#">Security</a></li>

<li><a href="#">Encryption</a></li>

<li><a href="#">Decryption</a></li>

<li><a href="#">Data Hiding</a></li>

<li><a href="#">Data Sharing</a></li>

</ul>

</div>

<div class="one\_quarter">

<h6 class="title">Techniques</h6>

<ul class="nospace linklist">

<li>

<article>

<p class="nospace">Key exchange protocols enable two or more parties to

establish a shared encryption key that they can use to encrypt</p>

</article>

</li>

<li>

<article>

<p class="nospace">sign data that they plan to

exchange. As key exchange schemes with certificates require some trusted authority</p>

</article>

</li>

</ul>

</div>

</div>

</footer>

</div>

<div class="wrapper row5">

<div id="social" class="hoc clear">

<div class="one\_half first">

<h6 class="title">Social Media</h6>

<ul class="faico clear">

<li><a class="faicon-facebook" href="#"><i class="fa fa-facebook"></i></a></li>

<li><a class="faicon-pinterest" href="#"><i class="fa fa-pinterest"></i></a></li>

<li><a class="faicon-twitter" href="#"><i class="fa fa-twitter"></i></a></li>

<li><a class="faicon-dribble" href="#"><i class="fa fa-dribbble"></i></a></li>

<li><a class="faicon-linkedin" href="#"><i class="fa fa-linkedin"></i></a></li>

<li><a class="faicon-google-plus" href="#"><i class="fa fa-google-plus"></i></a></li>

<li><a class="faicon-vk" href="#"><i class="fa fa-vk"></i></a></li>

<li><a class="faicon-youtube" href="#"><i class="fa fa-youtube"></i></a></li>

<li><a class="faicon-rss" href="#"><i class="fa fa-rss"></i></a></li>

</ul>

</div>

<div class="one\_half">

<h6 class="title">Join our community :</h6>

<form class="clear" method="post" action="#">

<fieldset>

<legend>Newsletter:</legend>

<input type="text" value="" placeholder="Type Email Here&hellip;">

<button class="fa fa-share" type="submit" title="Submit"><em>Submit</em></button>

</fieldset>

</form>

</div>

</div>

</div>

<div class="wrapper row6">

<div id="copyright" class="hoc clear">

<p class="fl\_left"> <a href="#"></a></p>

<p class="fl\_right"> <a target="\_blank" href="http://www.os-templates.com/" title="Free Website Templates"></a></p>

</div>

</div>

<a id="backtotop" href="#top"><i class="fa fa-chevron-up"></i></a>

<!-- JAVASCRIPTS -->

<script src="layout/scripts/jquery.min.js"></script>

<script src="layout/scripts/jquery.backtotop.js"></script>

<script src="layout/scripts/jquery.mobilemenu.js"></script>

<!-- IE9 Placeholder Support -->

<script src="layout/scripts/jquery.placeholder.min.js"></script>

<!-- / IE9 Placeholder Support -->

</body>

</html>

Admin\_userapprove.jsp

<%@ include file="include/dbconnect.jsp" %>

<%@page import="java.util.Random"%>

<%@page import="java.sql.ResultSet"%>

<html>

<head>

<title>ECC Data Sharing</title>

<meta charset="utf-8">

<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">

<link href="layout/styles/layout.css" rel="stylesheet" type="text/css" media="all">

<style type="text/css">

<!--

table, tr, td {

border: 3px white;

}

tr.noBorder td {

border: 0;

}

.style3 {color: #993333}

.style4 {font-size: 14px}

.style5 {color: #000000}

.style6 {

color: #000000;

font-size: 14px;

}

-->

</style>

</head>

<body id="top">

<div class="wrapper row0">

<div id="topbar" class="hoc clear">

<div class="fl\_left">

<ul class="nospace inline pushright">

<li><i class="fa fa-phone"></i> +00 (123) 456 7890</li>

<li><i class="fa fa-envelope-o"></i> info@domain.com</li>

</ul>

</div>

<div class="fl\_right">

<ul class="nospace inline pushright">

<li><i class="fa fa-sign-in"></i> <a href="#">Login</a></li>

<li><i class="fa fa-user"></i> <a href="#">Register</a></li>

</ul>

</div>

</div>

</div>

<div class="wrapper row1">

<header id="header" class="hoc clear">

<div id="logo" class="fl\_left">

<h1><a href="index.jsp">Ecc Data Sharing</a></h1>

</div>

<div id="search" class="fl\_right">

<form class="clear" method="post" action="#">

<fieldset>

<legend>Search:</legend>

<input type="search" value="" placeholder="Search Here&hellip;">

<button class="fa fa-search" type="submit" title="Search"><em>Search</em></button>

</fieldset>

</form>

</div>

</header>

</div>

<div class="wrapper row2">

<nav id="mainav" class="hoc clear">

<ul class="clear">

<li ><a href="admin\_home.jsp">Home</a></li>

<li><a href="admin\_ownerapprove.jsp">Owner Approve</a></li>

<li class="active"><a href="admin\_userapprove.jsp">User Approve</a></li>

<li><a href="index.jsp">Logout </a></li>

</ul>

</nav>

</div>

<div class="wrapper bgded" style="background-image:url('images/demo/backgrounds/ecc.png');">

<div id="pageintro" class="hoc clear">

<article>

<div class="overlay inspace-30 btmspace-30">

<h2 class="heading">Ecc Data Sharing</h2>

<p>Electronic health records possess the patient&#39;s medication details and their health history.</p>

</div>

</article>

</div>

</div>

<form action="" method="post" name="form1" id="form1" >

<p>&nbsp;</p>

<table width="81%" border="0" align="center">

<%

String uid=(String) session.getAttribute("uid");

ResultSet rs0 = stmt3.executeQuery("select \* from user where status='0' && report='0' ");

int s = 0;

while (rs0.next()) {

if (s == 0) {

%>

<tr>

<td height="53" colspan="8"><div align="center" class="style3">User Request : </div></td>

</tr>

<tr>

<td width="51" height="32"><h4 align="center" class="style1"><strong><span class="style1 style7 style4 style5"><em>Id</em></span></strong></h4></td>

<td width="114"><h4 align="center" class="style1 style7 style4 style5"><em><strong>Name</strong></em></h4></td>

<td width="114"><h4 align="center" class="style1 style7 style5 style4"><em><strong>Gender</strong></em></h4></td>

<td width="146"><h4 align="center" class="style1 style7 style5 style4"><em><strong>Mobile</strong></em></h4></td>

<td width="158"><h4 align="center" class="style1 style7 style4 style5"><em><strong>Gmail</strong></em></h4></td>

<td width="158"><h4 align="center" class="style1 style7 style6"><em><strong>Address</strong></em></h4></td>

<td width="158"><h4 align="center" class="style7 style1 style5 style4"><em><strong>Status</strong></em></h4></td>

<td width="158"><h4 align="center" class="style1 style7 style4 style5"><em><strong>Approved</strong></em></h4></td>

</tr>

<%

}

s++;

%>

<tr>

<td height="42"><div align="center"><span class="style6">

<% out.print(s);%>

</span></div></td>

<td><div align="center"><span class="style6">

<% out.print(rs0.getString("name"));%>

</span></div></td>

<td><div align="center"><span class="style6">

<% out.print(rs0.getString("gender"));%>

</span></div></td>

<td><div align="center"><span class="style6">

<% out.print(rs0.getString("mobile"));%>

</span></div></td>

<td><div align="center"><span class="style6">

<% out.print(rs0.getString("gmail"));%>

</span></div></td>

<td><div align="center"><span class="style5">

<% out.print(rs0.getString("address"));%>

</span></div></td>

<td><div align="center"><span class="style5">

<%

String sta=rs0.getString("status");

if(sta.equalsIgnoreCase("0"))

{

out.print("waiting");

}

else

{

out.print("approved");

}

%>

</span></div></td>

<td> <div align="center"><a href="approve\_user.jsp?fid=<% out.print(rs0.getString("id"));%>"> Approved</a></div></td>

</tr>

<%

}

%>

</table>

<p>&nbsp;</p>

<p>&nbsp;</p>

<p>&nbsp;</p>

</form>

<form action="" method="post" name="form1" id="form1" >

<p>&nbsp;</p>

<table width="81%" border="0" align="center">

<%

ResultSet rs = stmt4.executeQuery("select \* from user where report!='1' && cd='1' ");

int s1 = 0;

while (rs.next()) {

if (s1 == 0) {

%>

<tr>

<td height="50" colspan="8"><div align="center" class="style3">Approved Users : </div></td>

</tr>

<tr>

<td width="51" height="32"><h4 align="center" class="style1"><strong><span class="style7 style1 style4 style5"><em>Id</em></span></strong></h4></td>

<td width="114"><h4 align="center" class="style1 style7 style4 style5"><em><strong>Name</strong></em></h4></td>

<td width="114"><h4 align="center" class="style1 style7 style5 style4"><em><strong>Gender</strong></em></h4></td>

<td width="146"><h4 align="center" class="style1 style7 style5 style4"><em><strong>Mobile</strong></em></h4></td>

<td width="158"><h4 align="center" class="style1 style7 style5 style4"><em><strong>Gmail</strong></em></h4></td>

<td width="158"><h4 align="center" class="style1 style7 style4 style5"><em><strong>Address</strong></em></h4></td>

<td width="158"><h4 align="center" class="style7 style1 style5 style4"><em><strong>Status</strong></em></h4></td>

</tr>

<%

}

s1++;

%>

<tr>

<td height="42"><div align="center"><span class="style6">

<% out.print(s1);%>

</span></div></td>

<td><div align="center"><span class="style6">

<% out.print(rs.getString("name"));%>

</span></div></td>

<td><div align="center"><span class="style6">

<% out.print(rs.getString("gender"));%>

</span></div></td>

<td><div align="center"><span class="style6">

<% out.print(rs.getString("mobile"));%>

</span></div></td>

<td><div align="center"><span class="style6">

<% out.print(rs.getString("gmail"));%>

</span></div></td>

<td><div align="center"><span class="style6">

<% out.print(rs.getString("address"));%>

</span></div></td>

<td><div align="center"><span class="style6">

<%

String sta=rs.getString("report");

if(sta.equalsIgnoreCase("0"))

{

out.print("waiting");

}

else

{

out.print("approved");

}

%>

</span></div></td>

</tr>

<%

}

%>

</table>

<p>&nbsp;</p>

<p>&nbsp;</p>

<p>&nbsp;</p>

<p>&nbsp;</p>

</form>

<div class="wrapper row4 bgded overlay" style="background-image:url('images/demo/backgrounds/ecc1.jpg');">

<footer id="footer" class="hoc clear">

<div id="cta" class="group">

<div class="one\_third first"><i class="fa fa-map-marker"></i>

<p>Find us</p>

<p><a href="#">Google Maps</a></p>

</div>

<div class="one\_third"><i class="fa fa-phone"></i>

<p>Call us</p>

<p>+00 (123) 456 7890</p>

</div>

<div class="one\_third"><i class="fa fa-envelope-o"></i>

<p>Email us</p>

<p>info@domain.com</p>

</div>

</div>

<div class="group">

<div class="one\_quarter first">

<h6 class="title">ECC Data Sharing</h6>

<p>EHR generally

contains highly-sensitive and critical data related to patients, which is frequently shared

among clinicians, radiologists, healthcare providers, pharmacists, and researchers, for

effective diagnosis and treatment.</p>

</div>

<div class="one\_quarter">

<h6 class="title">Level 0</h6>

<ul class="nospace linklist">

<li><a href="#">Authentication Framework</a></li>

<li><a href="#">User Enrollment</a></li>

<li><a href="#">Key Destribution</a></li>

<li><a href="#">EHR sharing</a></li>

<li><a href="#">Key and Session Verification</a></li>

</ul>

</div>

<div class="one\_quarter">

<h6 class="title">Level 1</h6>

<ul class="nospace linklist">

<li><a href="#">Security</a></li>

<li><a href="#">Encryption</a></li>

<li><a href="#">Decryption</a></li>

<li><a href="#">Data Hiding</a></li>

<li><a href="#">Data Sharing</a></li>

</ul>

</div>

<div class="one\_quarter">

<h6 class="title">Techniques</h6>

<ul class="nospace linklist">

<li>

<article>

<p class="nospace">Key exchange protocols enable two or more parties to

establish a shared encryption key that they can use to encrypt</p>

</article>

</li>

<li>

<article>

<p class="nospace">sign data that they plan to

exchange. As key exchange schemes with certificates require some trusted authority</p>

</article>

</li>

</ul>

</div>

</div>

</footer>

</div>

<div class="wrapper row5">

<div id="social" class="hoc clear">

<div class="one\_half first">

<h6 class="title">Social Media</h6>

<ul class="faico clear">

<li><a class="faicon-facebook" href="#"><i class="fa fa-facebook"></i></a></li>

<li><a class="faicon-pinterest" href="#"><i class="fa fa-pinterest"></i></a></li>

<li><a class="faicon-twitter" href="#"><i class="fa fa-twitter"></i></a></li>

<li><a class="faicon-dribble" href="#"><i class="fa fa-dribbble"></i></a></li>

<li><a class="faicon-linkedin" href="#"><i class="fa fa-linkedin"></i></a></li>

<li><a class="faicon-google-plus" href="#"><i class="fa fa-google-plus"></i></a></li>

<li><a class="faicon-vk" href="#"><i class="fa fa-vk"></i></a></li>

<li><a class="faicon-youtube" href="#"><i class="fa fa-youtube"></i></a></li>

<li><a class="faicon-rss" href="#"><i class="fa fa-rss"></i></a></li>

</ul>

</div>

<div class="one\_half">

<h6 class="title">Join our community :</h6>

<form class="clear" method="post" action="#">

<fieldset>

<legend>Newsletter:</legend>

<input type="text" value="" placeholder="Type Email Here&hellip;">

<button class="fa fa-share" type="submit" title="Submit"><em>Submit</em></button>

</fieldset>

</form>

</div>

</div>

</div>

<div class="wrapper row6">

<div id="copyright" class="hoc clear">

<p class="fl\_left"> <a href="#"></a></p>

<p class="fl\_right"> <a target="\_blank" href="http://www.os-templates.com/" title="Free Website Templates"></a></p>

</div>

</div>

<a id="backtotop" href="#top"><i class="fa fa-chevron-up"></i></a>

<!-- JAVASCRIPTS -->

<script src="layout/scripts/jquery.min.js"></script>

<script src="layout/scripts/jquery.backtotop.js"></script>

<script src="layout/scripts/jquery.mobilemenu.js"></script>

<!-- IE9 Placeholder Support -->

<script src="layout/scripts/jquery.placeholder.min.js"></script>

<!-- / IE9 Placeholder Support -->

</body>

</html>

Approve \_owner.jsp

<%@page import="javapack.Crypt"%>

<%@page import="javapack.Mail"%>

<%@page import="java.util.Random"%>

<%@ include file="include/dbconnect.jsp" %>

<%

String mail="";

String id=request.getParameter("fid");

ResultSet rs0=stmt3.executeQuery("select \* from owner where id='"+id+"' ");

if(rs0.next())

{

mail=rs0.getString("gmail");

}

%>

<%

Random rnd = new Random();

Random rnd1 = new Random();

int number = rnd.nextInt(999);

// this will convert any number sequence into 6 character.

String ot= String.format("%03d", number);

session.setAttribute("ott", ot);

String reversed="";

byte[] strAsByteArray = ot.getBytes();

byte[] result = new byte[strAsByteArray.length];

// Store result in reverse order into the

// result byte[]

for (int i = 0; i < strAsByteArray.length; i++)

result[i] = strAsByteArray[strAsByteArray.length - i - 1];

reversed=new String(result);

out.print(reversed);

String ins = "update owner set report='"+reversed+"',cd=1='1' where id='"+id+"' ";

int n = stmt1.executeUpdate(ins);

Mail.SendMail(mail, "Your Activation Key",reversed,"");

if(n==1)

{

%>

<script language="javascript">

alert("Accept and Key Send Successful");

window.location.href="admin\_ownerapprove.jsp";

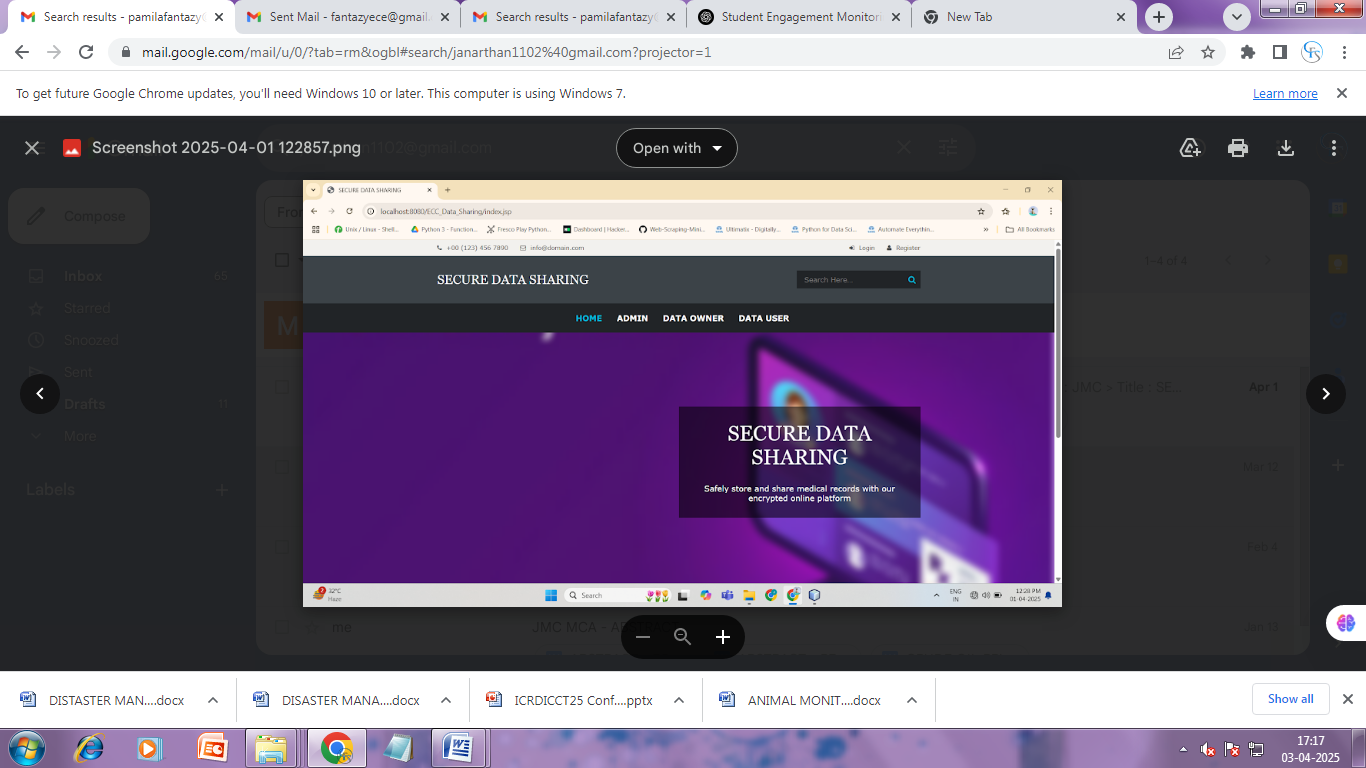
</script>

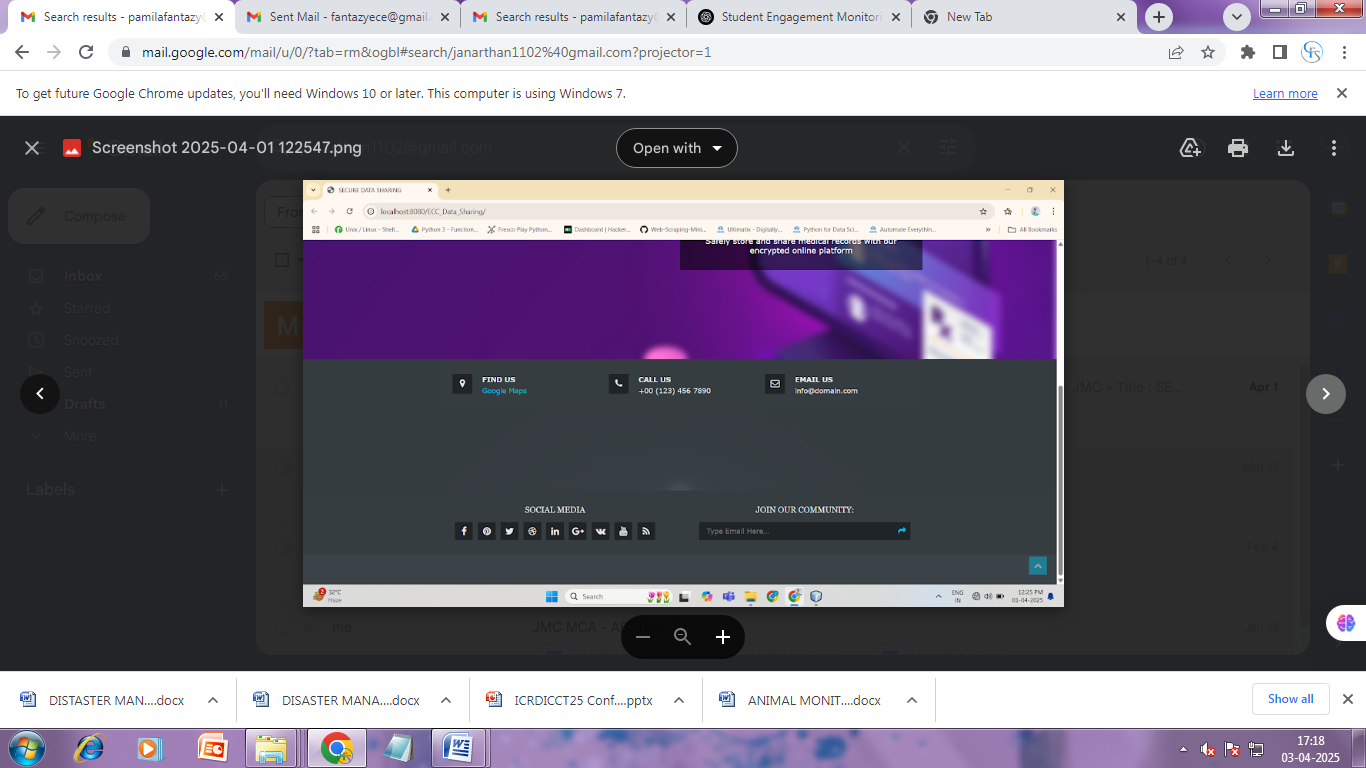
<%

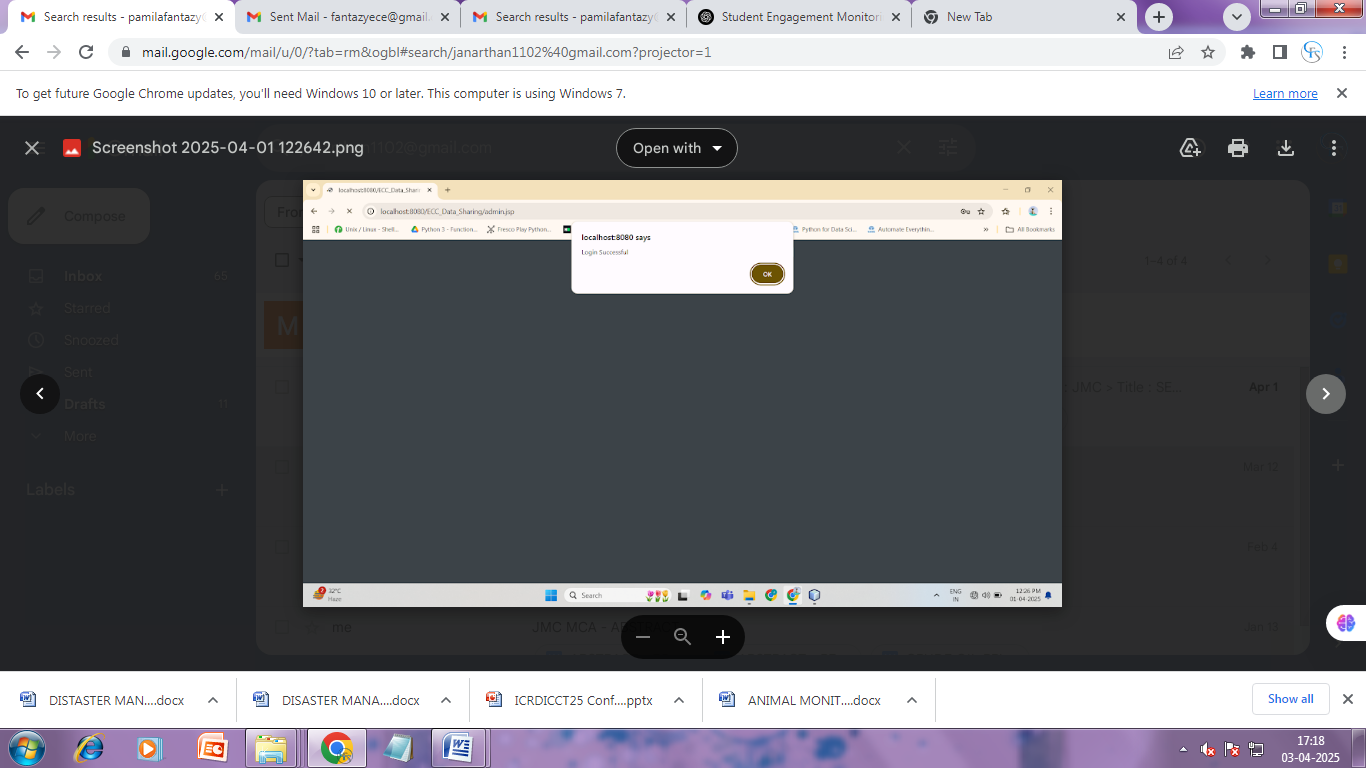
}

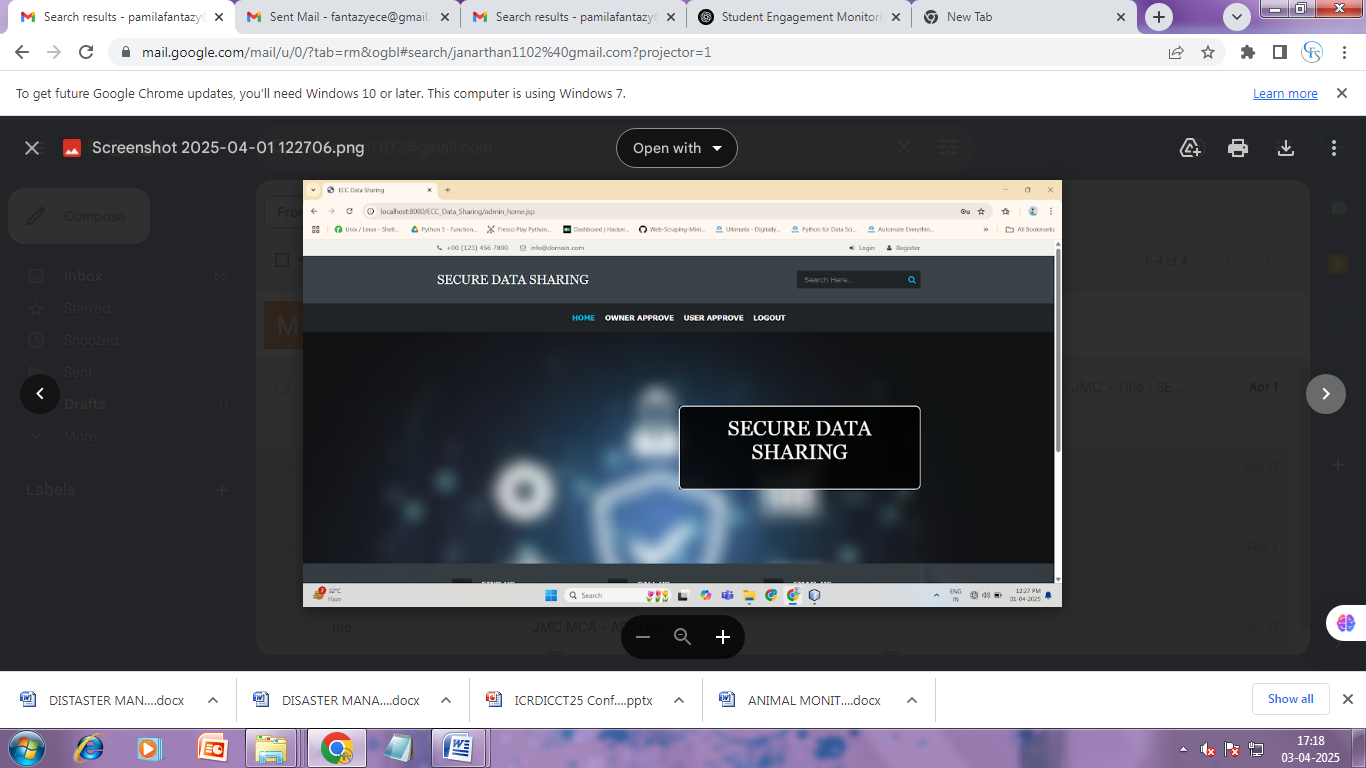
%>

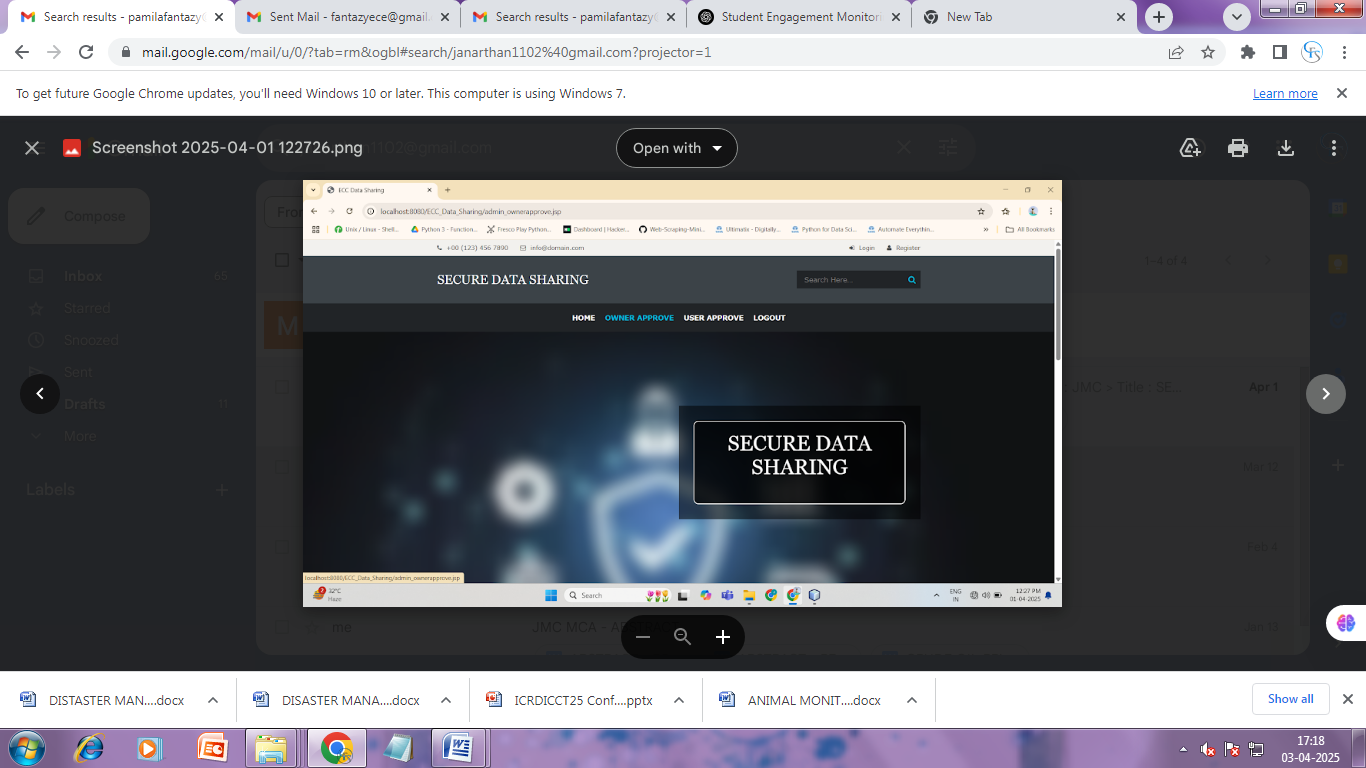
**9.2 OUTPUT SCREENSHOTS**

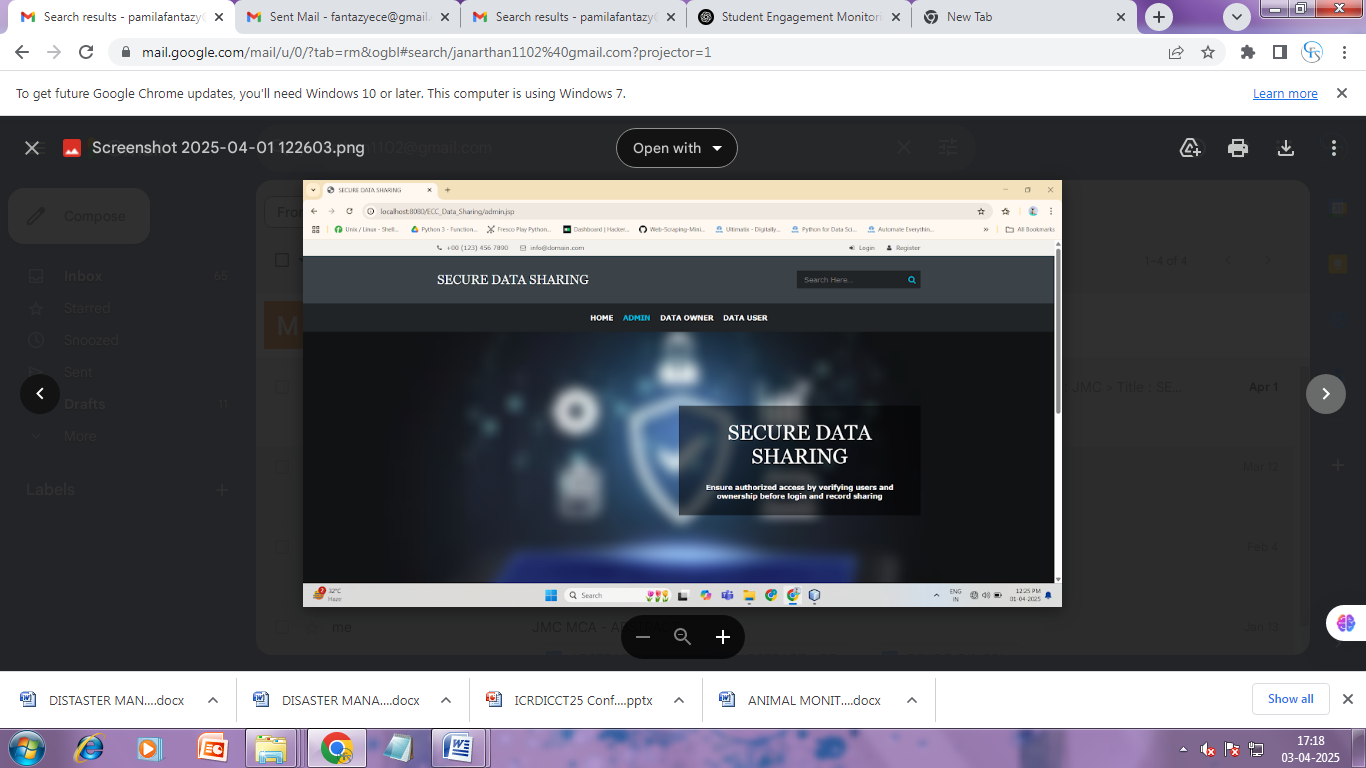
****

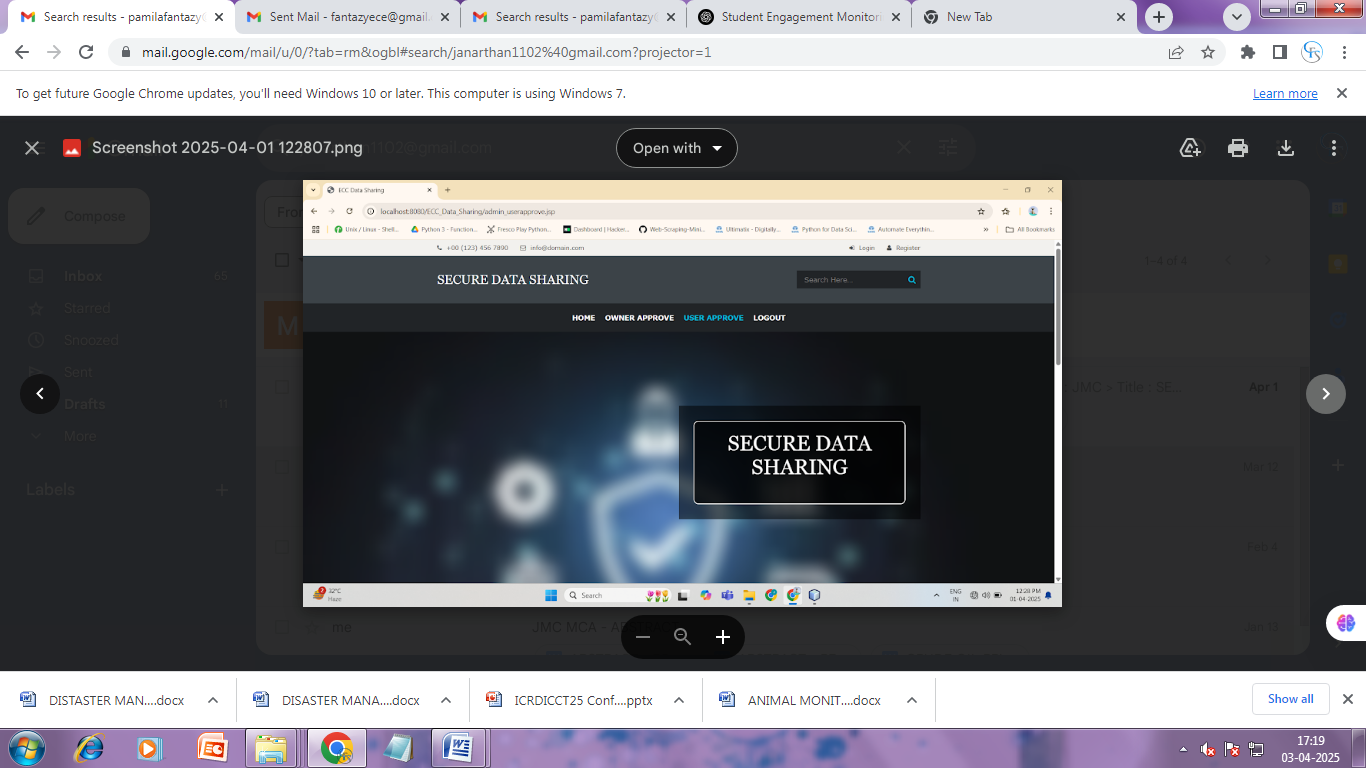
****

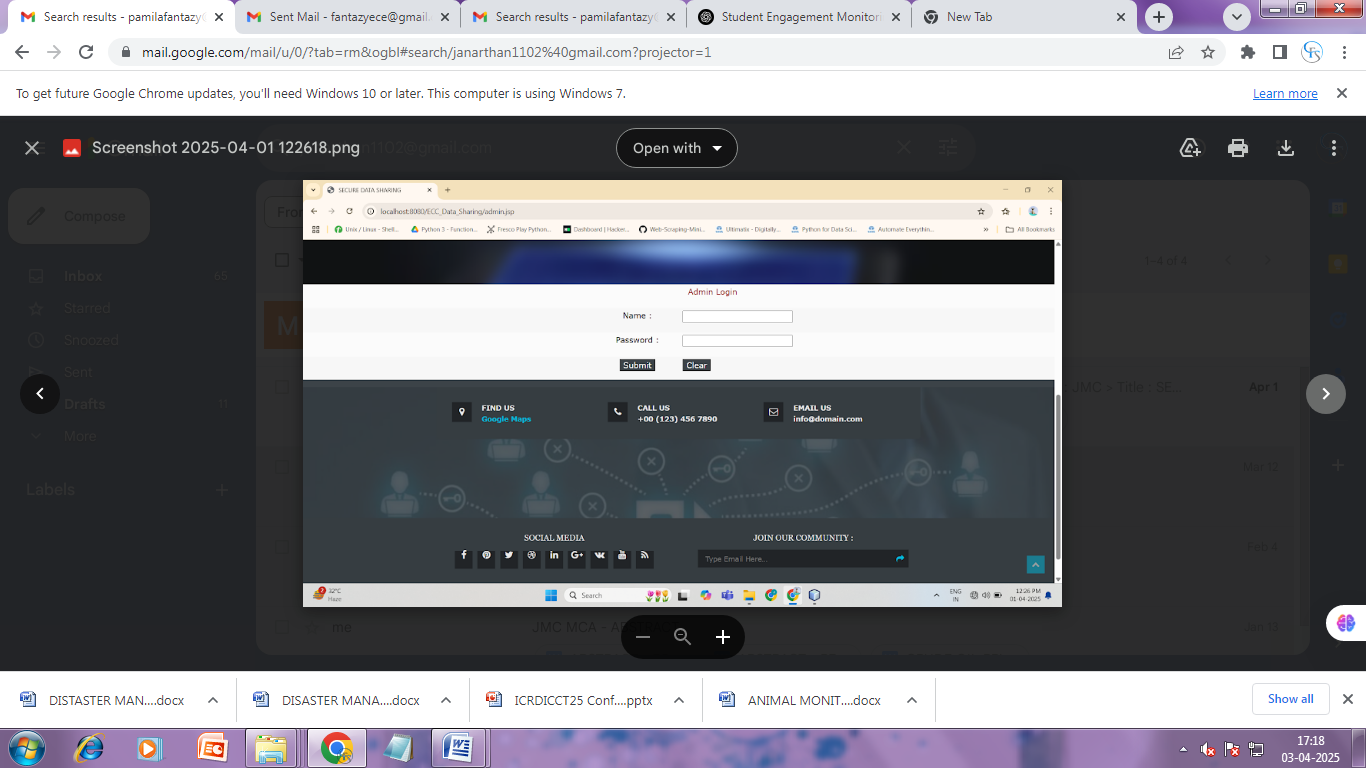
****

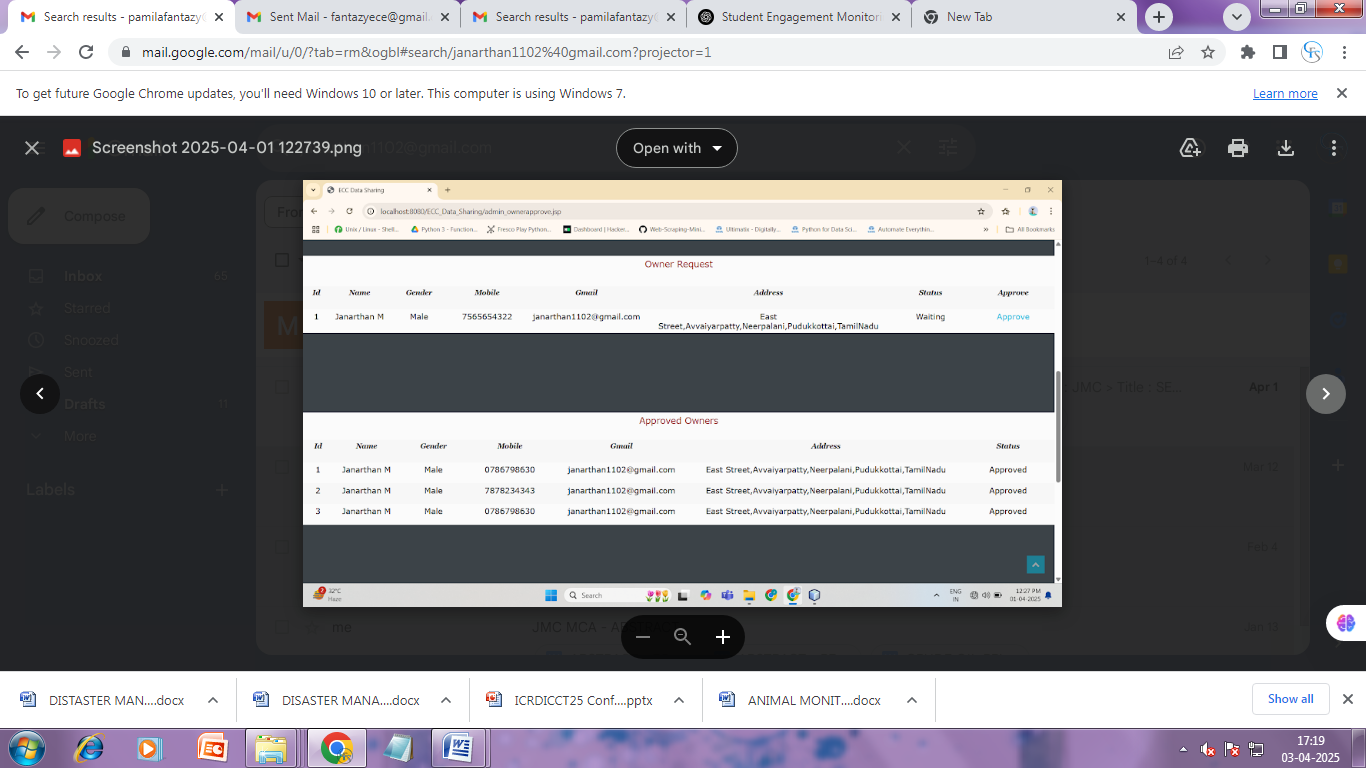
****

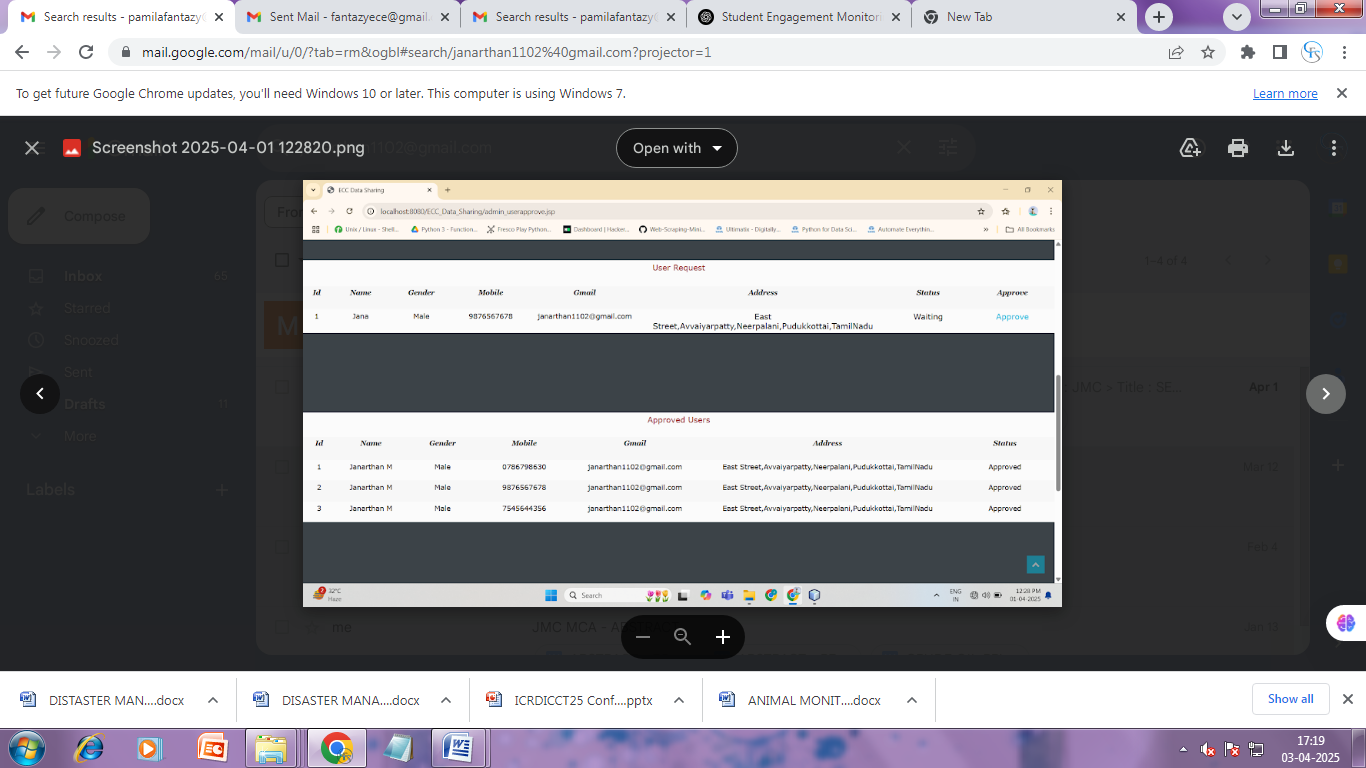
****

****

****

****

****

****