**IDEATION PLATFORM WITH INFORMATION SECURITY POLICIES**

A PROJECT REPORT

*Submitted by*

**Teja Paila [Reg No: RA1911042010119]**

**Bharadwaja Sarma [Reg No: RA1911042010070]**

*Under the Guidance of*

**Dr. Paul.T.Sheeba**

(Assistant Professor, Department of Data Science and Business Systems)

*In partial fulfillment of the Requirements for the Degree*

*of*

**BACHELOR OF TECHNOLOGY**

**COMPUTER SCIENCE AND BUSINESS SYSTEMS**



**DEPARTMENT OF DATA SCIENCE AND BUSINESS SYSTEMS**

**COLLEGE OF ENGINEERING AND TECHNOLOGY SRM INSTITUTE OF SCIENCE AND TECHNOLOGY KATTANKULATHUR – 603 203**

**MAY 2023**

Department of Data Science and Business Systems

**SRM Institute of Science & Technology**

###### Own Work Declaration Form

###### Degree/ Course : B.Tech in Computer Science and Business Systems

**Student Name** :Teja Paila and Bharadwaja Sarma

###### Registration Number :RA1911042010119, RA1911042010070

**Title of Work :**Ideation Platform With Information Security Policies

We hereby certify that this assessment complies with the University’s Rules and Regulations relating to Academic misconduct and plagiarism, as listed in the University Website, Regulations, and the Education Committee guidelines.

We confirm that all the work contained in this assessment is our own except where indicated, and that we have met the following conditions:

* Clearly references / listed all sources as appropriate
* Referenced and put in inverted commas all quoted text (from books, web, etc)
* Given the sources of all pictures, data etc. that are not my own
* Not made any use of the report(s) or essay(s) of any other student(s) either past or present
* Acknowledged in appropriate places any help that I have received from others (e.g. fellow students, technicians, statisticians, external sources)
* Compiled with any other plagiarism criteria specified in the Course handbook / University website

We understand that any false claim for this work will be penalized in accordance with the University policies and regulations.

|  |
| --- |
| **DECLARATION:** |
| We (RA1911042010119 and RA1911042010070) are aware of and understand the University’s policy on Academic misconduct and plagiarism and I certify that this assessment is my / our own work, except where indicated by referring, and that I have followed the good academic practices noted above. |
| RA19110420119 RA1911042010070 |



**SRM INSTITUTE OF SCIENCE AND TECHNOLOGY**

**KATTANKULATHUR – 603203**

**BONAFIDE CERTIFICATE**

Certified that the 18CSP462L project report titled “**IDEATION PLATFORM WITH INFORMATION SECURITY POLICIES”** is the bonafide work of **“Teja Paila [RA1911042010119] and Bharadwaja Sarma [RA1911042010070]”** who carried out the project work under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form part of any other thesis or dissertation on the basis of which a degree or award was conferred on an earlier occasion for this or any other candidate.

|  |  |
| --- | --- |
| DR. PAUL T. SHEEBA  **SUPERVISOR**  Assistant Professor  Department of Data Science and Business Systems | DR. M. LAKSHMI  **HEAD OF THE DEPARTMENT**  Department of Data Science and Business Systems |
| Signature of Internal Examiner | Signature of External Examiner |

**ABSTRACT**

Social networking sites are a staple of modern-day life. The social networking sites are used by millions of people to interact with family, friends, and share private or personal information. Social media platforms are regarded as reliable for communication needs, both personal and professional. Here is a project putting forth a strategy to foster an atmosphere where people can share their ideas and build businesses around them with the aid of a network or community. A collection of people who work in the same industry is referred to as a community in this context. This could be utilized to assist one another in developing their conceptions and enhancing their ideas. Individuals make up the majority of a social network, thus safeguarding them against false information and other users is crucial. Security features and network policies are implemented to accomplish this. Individuals make up the majority of a social network, thus safeguarding them against false information and other users is crucial. Security features and network policies are implemented to accomplish this. The basis of a network is made up of the same framework and structural components, such as users, community, privacy, security, and reliability, in the contemporary environment where different types of networks have been established for every imaginable function. In general, networks work to create a space for group interaction where members may express themselves and widen their circle of friends by connecting with others who share their perspective on an event or situation.

# **ACKNOWLEDGEMENTS**

We express our humble gratitude to **Dr. C. Muthamizhchelvan**, Vice- Chancellor, SRM Institute of Science and Technology, for the facilities extended for the project work and his continued support.

We extend our sincere thanks to Dean-CET, SRM Institute of Science and Technology, **Dr. T. V. Gopal**, for his invaluable support.

We wish to thank **Dr. Revathi Venkataraman**, Professor and Chairperson, School of Computing, SRM Institute of Science and Technology, for her support throughout the project work.

We are incredibly grateful to our Head of the Department**, Dr. M. Lakshmi** Professor, Department of Data Science and Business Systems, SRM Institute of Science and Technology, for her suggestions and encouragement at all the stages of the project work.

We want to convey our thanks to our program coordinator **Dr. E. Sasikala,** Professor, Department of Data Science and Business Systems, SRM Institute of Science and Technology, for her input during the project reviews and support.

We want to convey our thanks to our Project Coordinator, **Dr P. Rajasekar**, Assistant Professor, Panel Head, **Dr. A. Murugan**, Associate Professor and members, **Dr. R. Rajkumar**, Assistant Professor, **Dr. T. Karthick**, Assistant Professor and **Dr. S. Jeeva**, Assistant Professor, Department of Data Science and Business Systems, SRM Institute of Science and Technology, for their inputs during the project reviews and support.

We register our immeasurable thanks to our Faculty Advisor**, Dr. R Rajkumar,** Assistant Professor, Department of Data Science and Business Systems, SRM Institute of Science and Technology, for leading and helping us to complete our course.

Our inexpressible respect and thanks to our supervisor, **Dr. Paul T Sheeba,** Assistant Professor, Department of Data Science and Business Systems, SRM Institute of Science and Technology, for providing us with an opportunity to pursue our project under her mentorship. She provided us with the freedom and support to explore the research topics of our interest. Her passion for solving problems and making a difference in the world has always been inspiring.

We sincerely thank the Data Science and Business Systems staff and students, at SRM Institute of Science and Technology, for their help during our project. Finally, we would like to thank our parents, family members, and friends for their unconditional love, constant support, and encouragement.

**Teja Paila [RA1911042010119]**

**Bharadwaja Sarma [RA1911042010070]**

### **TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CHAPTER**  **NO** | **TITLE** | **PAGE NO** |
|  | **ABSTRACT** | iv |
|  | **LIST OF FIGURES** | ix |
|  | **LIST OF SYMBOLS AND**  **ABBREVIATIONS** | x |
| **1** | **INTRODUCTION** | 1 |
|  | 1.1 Social Network | 1 |
|  | 1.2 Purpose of the project | 2 |
|  | 1.3 Motivation of the project | 3 |
|  | 1.4 Information Security policies | 3 |
|  | 1.5 Principle of Social Engineering | 4 |
|  | 1.6 Community Energy Initiatives (CEI) | 5 |
|  | 1.7 Gender difference in Social Network | 6 |
|  | 1.8 Structure of the Report | 10 |
| **2** | **LITERATURE STUDY** | 11 |
|  | 2.1 Bell-LaPadula Security Policies Using RBA | 11 |
|  | 2.2 Security threats and strategies for cyber attacks | 12 |
|  | 2.3 Technology to reduce social engineering | 13 |
| **3** | **METHODOLOGY & IMPLEMENTATION** | 15 |
|  | 3.1 Bella-LaPadula | 15 |
|  | 3.2 Biba Model | 17 |
|  | * 1. Clark Wilson Model | 18 |
|  | * 1. Modules | 19 |
|  | * 1. Implementation      1. Registration Page      2. Login Page      3. Chatting | 20  21  23  25 |
| **4** | **RESULTS AND DISCUSSION**  4.1 Female Users  4.2 Male Users | 31  28  31 |
| **5** | **CONCLUSION**  5.1 Conclusion  5.2 Future Enhancements | 34  34  35 |
|  | REFERENCES | 36 |
|  | APPENDIX 1 | 38 |
|  | APPENDIX 2 | 43 |
|  | PAPER PUBLICATION STATUS | 66 |
|  | PLAGIARISM REPORT | 67 |

### **LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
|  | Social Engineering Life Cycle | 4 |
|  | CEI working model in a network | 8 |
|  | Bell-Lapadula | 16 |
|  | Biba Model | 17 |
|  | Architecture Diagram | 20 |
|  | Registration page snippet | 21 |
|  | Database Image | 21 |
|  | Table of the Database | 22 |
|  | Table of the Database | 22 |
|  | Login page screenshot | 23 |
|  | Flow Chart | 24 |
|  | Activity Diagram | 25 |
|  | Chatting Login page screenshot | 26 |
|  | List of friends | 26 |
|  | Sample chatting | 27 |
|  | Female user account’s page snippet | 28 |
|  | Female user account’s page snippet | 28 |
|  | Female user account’s page snippet | 29 |
|  | Female user account’s page snippet | 30 |
|  | Male user account’s page snippet | 31 |
|  | Male user account’s page snippet | 32 |
|  | Male user account’s page snippet | 32 |
|  | Full-Stack | 41 |

### **LIST OF SYMBOLS AND ABBREVIATIONS**

|  |  |
| --- | --- |
| **IPFS** | InterPlanetary File System |
| **GUI** | Graphical User Interface |
| **DAPP** | Decentralised Application |
| **HTTP** | Hypertext Transfer Protocol |
| **CID** | Content Identifier |
| **SC** | Smart Contract |
| **DNS** | Domain Name System |
| **GPS** | Global Position System |
| **POW** | Proof-of-Work |
| **IC** | Intelligent Contract |
| **HTML** | Hyper Text Markup Language |
| **CSS** | Cascading Style Sheets |
| **SQL** | Structured Query Language |
| **CEI** | Community Energy Initiatives |
| **OTP** | One Time Password |
| **DP** | Display Picture |
| **RBAC** | Role Based Access Control |
| **DDOS** | Distribute Denial of Service |
|  |  |

**CHAPTER 1**

**INTRODUCTION**

1. **Social Network**

Humans are social animals, and interpersonal interactions and dialogue are fundamental to who we are. The urge to communicate still exists in the digital age, but how humans communicate has changed. Information security regulations are being used to safeguard user privacy and safeguard communications. Facial recognition is one of the features we are concentrating on adding to help female users feel more comfortable and inspired to share their ideas.

The internet is a network of connected computers and servers on a local, regional, and international scale. A component or feature of the internet called social networks enables people to interact with their friends and family. Social networks are seen as a collection of web-based applications that share information among one another in order to make it easier for users to meet new people and join groups where they can converse or share information relevant to their daily lives.

Social networking refers to using social media platforms to engage with current and future consumers in order to boost sales and grow your business. Facebook, YouTube, and Twitter are the social networking sites that people use the most. LinkedIn, Instagram, Pinterest, and Snapchat are a few other well-known social networking services. The large number of significant businesses have employed social media consultants or marketers to boost in the promotion of their products since social networking has demonstrated its efficacy as a marketing strategy.

The expense of any advertising may be significantly decreased by using social networking for marketing. Sponsored advertisements on social media platforms like Facebook are sometimes far more affordable than those in more established media, like radio or television, and frequently have the added benefit of being able to reach a larger audience.

For new, small enterprises with little money for advertising, social networking may be very beneficial. Some companies could be able to completely ignore paid advertising and advertise their goods by simply spending the required time and energy to posting content about them on social networking websites.

1. **Purpose of the project**

People that have amazing ideas but limited exposure are eager for all the assistance they can get. Yet are unable to locate trustworthy sources or persons nearby. In the current environment, women struggle to locate a safe and trustworthy setting where they may share their views and look for work prospects. There are various social media sites, such Facebook, LinkedIn, and others, that we may use to introduce oneself, but they don't pay much attention to the security of the data that is accessed through them. The original creator of the idea, who could be of any gender, is unable to locate an opportunity to publish it on social media that is trustworthy and secure against replicating the idea.

To express their ideas and seek assistance in daily life, humans require assistance and trustworthy individuals. Women are unable to locate a place where they can trust every communication they receive since profile authentication is not happening as often as it should. the development of a social network where users may freely share their views and ideas without worrying about being scammed, having phony accounts created, or having their ideas stolen.

The goal of the project is to provide women with a safe networking environment where they can promote themselves and their ideas. by including the IS models as part of the website development process. Users can propose their ideas and offer as much assistance as they can from anywhere in the world. The main goal is to give consumers a secure network by preventing false accounts on our website with a rigorous registration procedure. And make an effort to increase members' involvement in the necessary work.

1. **Motivation of the project**

Women with brilliant ideas but limited exposure should use all the assistance they could get. Women struggled to find a trustworthy environment in which to share their ideas. They might showcase their concepts, undertakings, and work samples on our website and share them with the globe.

1. **Information security policy**

Information security models are essential for organizations to effectively implement and enforce their information security policies. These models provide a framework for designing and implementing security controls to protect against various threats and vulnerabilities. There are several types of security models, including access control models, computing models, and computational models.

Access control models define the rules and permissions required to access specific resources or data within an organization. The most common access control model is the access control matrix, which maps users to the resources they are authorized to access. Other access control models include role-based access control and attribute-based access control.

Computing models provide a framework for analyzing and mitigating security risks associated with the design and operation of computer systems. Examples of computing models include the Bell-LaPadula model, which focuses on confidentiality, and the Biba model, which focuses on integrity.

Computational models use mathematical and logical methods to analyze and evaluate the security of computer systems. These models are often used to test the effectiveness of security controls and to identify potential vulnerabilities in system design and operation.

Overall, information security policies and models are crucial components of any organization's cybersecurity strategy. They provide a framework for protecting sensitive data, maintaining customer trust, and avoiding costly cyberattacks.

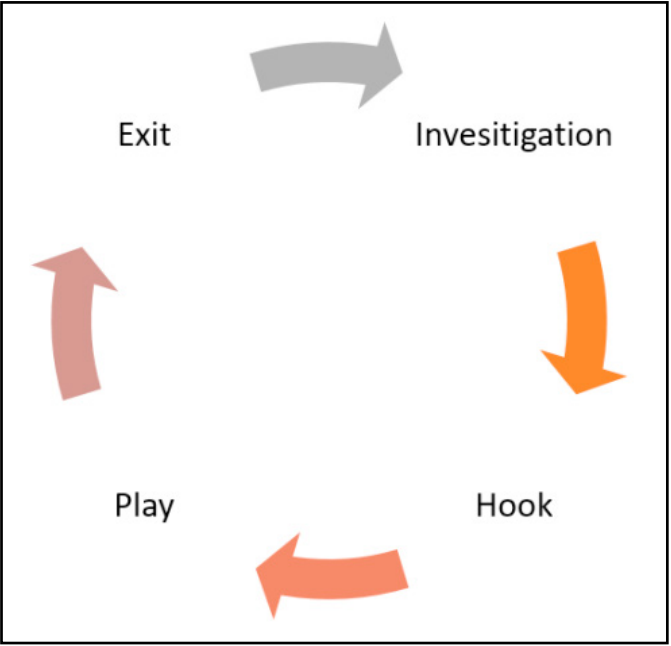
1. **PRINCIPLE OF SOCIAL ENGINEERING:**

Social engineering is the practice of manipulating and deceiving individuals into divulging confidential or sensitive information or performing actions that may be harmful to themselves or others. It is a technique that has been used by hackers and cybercriminals to gain unauthorized access to systems, steal data, and cause damage to organizations.

Scams involving social engineering concentrate on how people feel, act, and think. Once an attacker is aware of what motivates a user's activities, they are simple to control. Most social engineering frauds rely on open communication between the perpetrator and the target. The attacker would try to persuade the user to compromise themself rather than utilizing brute force techniques to break the data. The below Fig.1 explains the life cycle of social engineering.

The steps in a typical social engineering life cycle are as follows:

• Research: After selecting a victim, the assailant will learn as much as possible about them before deciding on an attack strategy.



1. *Social engineering life cycle*

•Hook: By building a rapport and winning the victim's trust, the attacker will approach them more closely.

•Play: After a relationship has been established, the assailant will manipulate the victim to get the information they need.

•Exit: The attacker will cut off contact with the victim after they have the required data or the user has taken the desired action. At that point, they will move on to a new victim

Generally large section of the public use a single password across all the utility, if incase a hacker gets successful in hijacking or socially engineering one’s personal email password, then they get the access to that users personal contact list. Attacker will break up contact with the victim and go on to a different one. Because most people use the same password for all of their accounts, a criminal who successfully hacks or socially engineers one person's email password is likely to have access to the users social networking contacts as well. As a result, it is prudent to use distinct passwords for each account

It is important to be aware of the principles of social engineering to protect yourself and your organization from potential threats. This includes being vigilant and skeptical of unsolicited emails or phone calls, verifying the identity of individuals who claim to be in positions of authority, and maintaining awareness of the tactics that social engineers may use to manipulate their targets.

Incorporating security policies and training employees on how to identify and respond to social engineering attacks can also help to mitigate the risk of data breaches and other security incidents. By building a culture of security and promoting best practices, organizations can create a safer and more secure environment for their employees and customers**.**

**Types of Social Attacks:**

1. Phishing:

Phishing is a cyberattack that exploits personal communication channels including email, phone, SMS, social media, and others to trick victims into opening dangerous links, downloading malicious files, or divulging sensitive data like users passwords, account details etc.

The most famous phishing attacks frequently make absurd requests for someone's financial information, such as a member of the royal family. The phishing fraud of today is considerably more complex, though. A cybercriminal will frequently pretend to be a company, service provider, or governmental agency in order to get private information such email addresses, phone numbers, the user's date of birth, or names of family members.

Phishing is one of the most common types of cyberattacks, and its frequency is on the rise. After COVID-19, all types of cyberattacks—including phishing attacks—dramatically increased. During the lockdown, people frequently spent more time online and experienced heightened emotions, which together created the perfect environment for a successful phishing attempt. Phishing was the most prevalent type of cybercrime in 2020, according to the FBI, with incidents nearly tripling from 2019.

1. Whaling:

A sort of phishing assault known as a whaling attack uses intimate conversation to access a user's device or personal data.

The degree of personalization is what distinguishes phishing from whaling. Whaling assaults target a single individual, usually a senior executive, in contrast to phishing attempts, which are impersonal and may be duplicated for millions of people. This kind of attack necessitates thorough investigation of the target, which is typically accomplished by looking into their online presence and other public behaviors. This extensive research leads to more sophisticated outreach efforts and a greater chance of success.

While whaling assaults initially involve more planning and preparation, they can result in enormous gains because the targets often have access to very valuable data or the necessary funds to further a ransomware campaign.

1. Diversion Theft:

A cyberattack that started offline is called diversion theft. A courier is tricked into picking up or dropping off a delivery at the wrong place, delivering the wrong cargo, or delivering the package to the wrong person in this attack. Since then, conversion theft has been transformed into an online scam. By fooling the user into transmitting confidential information to the incorrect recipient, the hostile actor takes sensitive data.

This attack type frequently uses spoofing, a method employed by hackers to pose as a reputable or well-known source. False emails, calls, websites, emails, DNS spoofing, GPS spoofing, and other methods are all examples of spoofing.

1. Honeytrap:

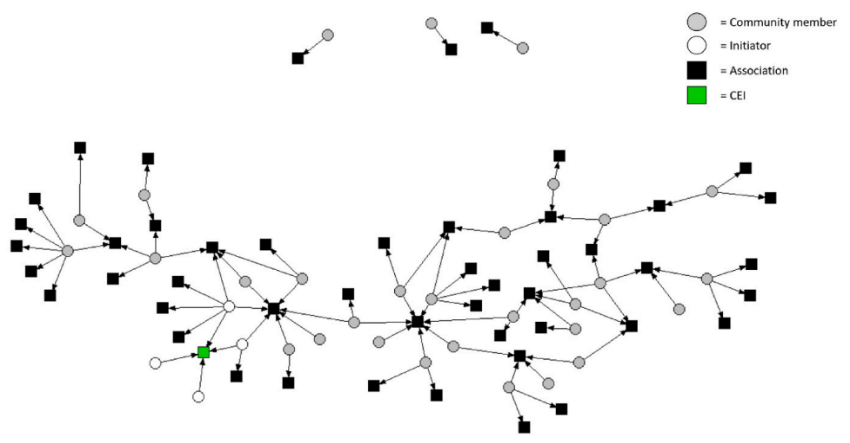
An online dating user or someone using social media who is looking for love is the target of a honeytrap attack, a social engineering tactic. By thinking of a fake identity and try’s to develops a bogus social profile, then they thief befriends to the victim. On the process of developing time, the criminal exploits the connection and connives the victim to gain money or could steal personal data, or could even introduce malware.

1. **Community Energy Initiatives (CEI):**

Typically, one or more community members—referred to as initiators—take the initiative to establish a CEI. They take on the "start-up costs" by starting a process that might result in a critical mass of community members who are willing to participate. The dynamics of collective action and social movements are similar to those of CEIs in this regard: establishing CEI & advancing it over past the point of success is a "lumpy" and a problem that is requiring a significant initial commitment of efforts. CEIs may wither away below the threshold, but once they cross it, they may spread similarly to step-level public goods. The ability of the initiators to involve other community members—people who reside within the community in which an initiative is embedded—is one of the key obstacles to putting up a successful CEI.

The emotional intensity, reciprocity, level of intimacy, and frequency of touch can all affect how strong a bond is. One can distinguish between strong and weak relationships, such as those between close friends and acquaintances as we can view in the below Fig.2. While weak links are important on a structural level because they connect otherwise isolated sections of a network, they are also significant on a relational (dyadic) level because they increase the likelihood that people may get new information. Therefore, it is believed that weak ties offer access to a variety of external resources, fresh concepts, and knowledge. Weak ties have been suggested to promote coordination of group action and to speed up diffusion processes, such as the adoption of new technology.

Strong ties demand frequent social contact and are frequently seen in more homogeneous, close-knit groups. They promote spread because, in addition to providing information, they also foster reciprocity, trust, social support, and the ability to exert social pressure. It has also been demonstrated that close relationships are crucial for the emergence of collaboration in institutions for collective action more generally. As a result, we anticipate that strong direct linkages to initiators, as opposed to weak direct relationships, will have a special impact on participation in a CEI.



1. *CEI working model in a network*

Not that weak direct links is unimportant—far from it. However, recognizing the value of close relationships takes into account the relative weight of social support vs knowledge in inspiring action.

Generally, community members with more associational memberships are more likely to participate. This implies that merely belonging to other associations within the community is more significant than developing long-term relationships with initiators through these associations. Thus, it would appear that network range, in addition to degree, is significant in enhancing the diversity of interactions within the community. However, since extended ties and the number of associational memberships is relatively closely connected, their impacts may partially cancel one another out.

Findings are in accordance with those of earlier studies, which suggest that people might participate not because of only they are been driven to engage in developing sustainable energy practices but even because they are motivated to become more involved in their local communities.

People are drawn into CEIs through others in their immediate social network who are already involved, according to a preliminary conclusion drawn from these findings, which implies that a community-led approach may in fact be partially associated with "the ability to leverage local social networks to achieve change"

1. **Gender difference in social network:**

Gender differences in social networks refer to the varying behaviors of male and female users on different aspects of social networking sites. Female users tend to be more affected by the effects of social networking sites, which leads to the need for security requirements for female users. To address this, social networking sites can give female users more control over their profiles, such as the ability to accept friend requests and delete users from their friends list.

Social cognitive theory of gender role development suggests that gender conceptions and role development are influenced by other social factors, such as consensus from one's immediate social networks and mass media, and implicit sex difference. Gender stereotypes, which are present in a wide variety of elements, influence the perception, assessment, and treatment of males and females in their behaviors.

Research has shown that gender differences are also present in computer-mediated communication, such as emails and text messages. Women tend to use emails to establish close relationships, talk about personal matters, and feel satisfied. Women frequently use social networking services to maintain close links and acquire social information about close and distant networks, whereas males typically use social networking services to obtain data of a broad character.

Gender homophily is another aspect that aids in the development of social relationships. Women tend to have slightly more female friends than men and are more inclined to choose them as close friends. Complex reasons for gender differences in social networks include both biological and social constructs, contributing to gender stereotypes, which are the result of the distribution of men and women in various social positions, especially in home and work responsibilities

1. **STRUCTURE OF THE REPORT**

The report is organized as follows: Chapter 2 provides a literature review on the topic, while Chapter 3 outlines the proposed methodology and its implementation. Chapter 4 presents the results. The report's conclusion and future enhancements are presented in Chapter 5, followed by the references. Additionally, an appendix is included that contains the program code, the paper publication status, and the plagiarism report, all located after the references Chapter 5.

**CHAPTER 2**

**LITERATURE STUDY**

Social network services are web-based platforms that enable users to establish virtual connections with others who share similar interests and backgrounds. These services facilitate the process of finding new communities and friends [13]. To generate and share data on social networks, various methods are employed. The proposed technique in this study presents a novel approach to enhance the structure of social networks and improve their security components, including accessibility, availability, and reliability. The architecture of multiple systems in online social networks (OSNs) includes client-server and peer-to-peer models [2].

Various studies have focused on analyzing the content of social networks and improving user security through the use of different models, protocols, mechanisms, and algorithms [1]. It is crucial to understand the different types of threats that exist in the network to help people become more aware of their surroundings. This research paper proposes a novel approach to enhancing social media security by introducing a crowd computing framework and hierarchical structure for social networks [4]. The **Bell-LaPadula** model is incorporated into the network to create a secure and reliable environment, particularly for female users.

1. **Bell-LaPadula Security Policies Using RBA**

A Bell-LaPadula policy is a security policy that combines both multi-level security and discretionary access control policies. This policy ensures the confidentiality of information while also maintaining the flexibility of access control policies. In order to enforce a Bell-LaPadula policy, a subject is granted access to an object only if the subject is authorized to access the object by both the multi-level security policy and the discretionary access control policy. This policy helps to ensure that only authorized individuals have access to sensitive information.

"The Modeling of Bell-LaPadula Security Policies Using RBA" is a research paper that explores the application of Role-Based Access Control (RBAC) to model the Bell-LaPadula security policies. The paper was written by Hossain et al. and was published in the Journal of Computer Science and Technology in 2009.

The paper begins by discussing the limitations of the traditional Bell-LaPadula model, which uses a hierarchical security classification system to control access to information. The authors argue that RBAC can provide a more flexible and scalable approach to enforcing security policies, particularly in large and complex systems.

The paper then presents a formal model for RBAC-based Bell-LaPadula security policies, which defines the roles, permissions, and constraints that govern access to information. The authors demonstrate how this model can be used to enforce a range of security policies, including mandatory access controls, discretionary access controls, and role-based access controls.

The paper also describes a case study in which the RBAC-based Bell-LaPadula model is applied to a real-world system, specifically an enterprise resource planning (ERP) system. The authors demonstrate how the RBAC model can be used to control access to sensitive data and ensure compliance with regulatory requirements.

Overall, the paper provides a detailed and thorough exploration of the use of RBAC to model Bell-LaPadula security policies. It highlights the benefits of RBAC over traditional security models, and provides a practical example of how this approach can be applied in real-world settings. The paper is a valuable resource for researchers and practitioners interested in security policy modeling and RBAC [16].

1. **Security Threats and Strategies for Cyber Attacks**

"AI Empowers Security Threats and Strategies for Cyber Attacks" is another research paper that explores the application of artificial intelligence (AI) in cyber-attacks and proposes strategies to mitigate the associated security threats. The paper was written by Muneer et al. and was published in the Journal of Computer Science and Technology in 2019[6].

The paper begins by discussing the increasing use of AI in various domains, including cyber-attacks. The authors argue that AI can be used to automate and enhance various aspects of cyber-attacks, such as reconnaissance, evasion, and attack delivery.

The paper then proposes several strategies to mitigate the security threats posed by AI-powered cyber-attacks. These strategies include enhancing security measures and defenses, such as intrusion detection and prevention systems, as well as increasing awareness and education about AI-powered attacks among security professionals and end-users.

The paper also presents a case study in which the proposed strategies were applied to mitigate the security threats posed by a specific type of AI-powered attack, namely adversarial attacks on machine learning systems. The authors demonstrate that the proposed strategies were effective in reducing the success rate of these attacks and increasing the resilience of the targeted machine learning systems.

1. **Technology to Reduce Social Engineering**

The paper begins by discussing the increasing importance of social media as a platform for communication, information sharing, and business operations, and the corresponding rise in social engineering attacks. The authors argue that social engineering attacks often exploit human vulnerabilities, such as lack of awareness or training, to gain unauthorized access to information or systems [12].

The paper then proposes a combination of education and technology as a solution to reduce social engineering risks and damage. The authors argue that education and training can improve awareness and behavior of social media users, while technology can provide additional layers of security and monitoring to prevent and detect social engineering attacks.

The paper also presents a case study in which a combination of education and technology was used to reduce social engineering risks in a large organization. The authors describe the implementation of a security awareness program, which included training and education for employees, as well as the deployment of a social engineering detection and prevention system. The authors demonstrate that the combination of education and technology was effective in reducing the number and severity of social engineering attacks in the organization. The number of people using social network for stealing personal information of users, using phishing technique, so every user in the network has to be more vigilant to protect their information [7].

The paper also highlights the need for ongoing training and awareness programs to keep users informed about new social engineering tactics and how to avoid them. Additionally, the authors stress the importance of creating a security culture within organizations, where security is seen as everyone's responsibility and not just that of the IT department [9].

When trying to investigate the part of social network in effecting the user's choice on to whether to be a part of communal activity. Discussing about engagement of members is critical part for the success of a communal energy initiative and this leads to main question on how the initiators of a program can reach the community members and stimulate their involvement [10][15].

Studies are even trying to investigate the role of social networks on how individual’s decisions are been influenced on trying to participate of community energy initiative. Later we are discussing about engagement of community members is crucial for the success of a CEI and thus a key question is how the initiators can reach community members and stimulate involvement [3]. Taking results of this to prove how greatly a community can impact the network to be moving forward. How well it can be initiated and how an initiated program is been affected by the associated individuals [8].

**CHAPTER 3**

**METHODOLOGY AND IMPLEMENTATION**

1. **Bell-LaPadula:**

This is an information security model which is also referred as a multi-level model, which was proposed for implementing access control in military applications. In these models there are two main parts one subjects and the other objects which are segregated into different security levels. The subject can access only objects at specific level determined by his access level.

The levels of classification are designed to protect information (or) data from unauthorized discloser.

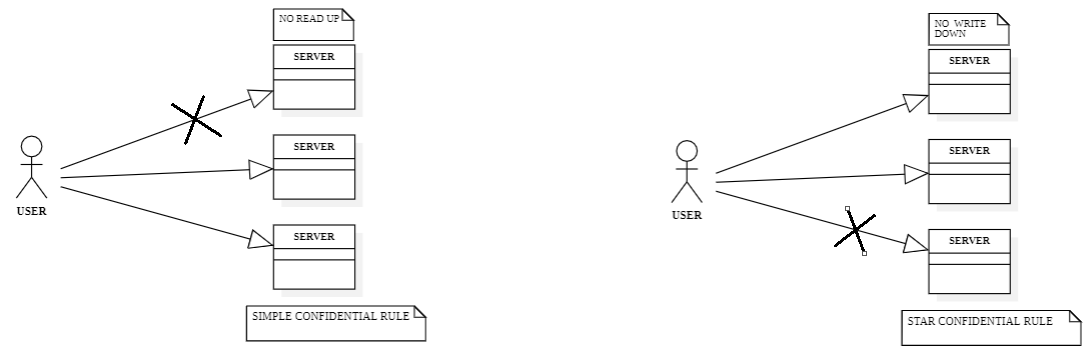
Simple confidential rule: In this the users (or) subjects can only **read** the data on the same level of access and the lower level of access but can’t read data to the upper level of access. This rule is also referred as **no read up** rule.

Star confidential rule: In this the users (or) subjects can only **write** the data on the same level of access and the upper level of access but can’t write data to the lower level of access. The rule is termed as **no write down** rule.

This is using these rules to improve the confidentiality of the data and users. **Confidentiality** implies that the protection of the data from being accessed by an unauthorized user. Only real users can access their personal information. The main responsibility of confidentiality is stopping information from getting into the inappropriate user’s hands.

The Bell-LaPadula model was one of the earliest modern security models to be created, which makes it important. As a result, it has influenced the creation of various security models. The model's lattice-based security model structure, which was novel at the time of its inception, adds further significance.

An essential safety tool, the Bell-LaPadula model offers a variety of features. The concept, which is used to safeguard information from unauthorized access, first establishes a set of security levels. By specifying a set of access rules that specify how individuals can access objects at various security levels, the model offers a framework for managing access to information at various security levels. Last but not least, the approach may be applied to audit information access and make sure that no unapproved access takes place.



1. *Bell-Lapadula Model*

In the above Fig.3 we are talking about the features of the Bell-LaPadula Model.

SIMPLE CONFIDENTIAL RULE: In this the users (or) subjects can only READ the data on the same level of access and the lower level of access but can’t read data to the upper level of access. This rule is called NO READ UP rule.

STAR CONFIDENTIAL RULE: In this the users (or) subjects can only WRITE the data on the same level of access and the upper level of access but can’t write data to the lower level of access. This rule is called NO WRITE DOWN rule.

This is using these rules to improve the confidentiality of the data and users. Confidentiality refers to the protecting the data from unauthorized access. Only legitimate users can access sensitive information. The main goal of confidentiality is to stop information from getting into the wrong hands.

1. **Biba Model:**

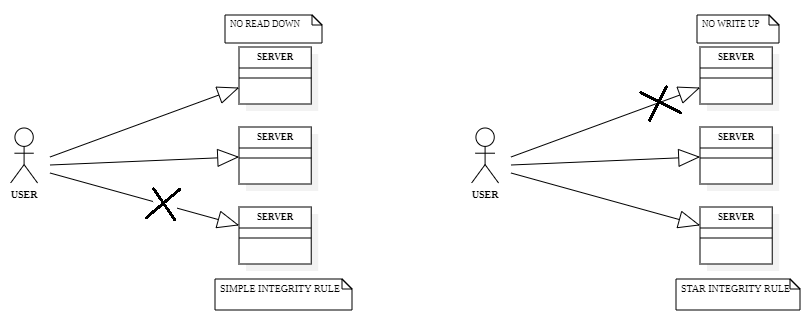
The Biba model was given this name in honour of its creator, Kenneth J. Biba. Information integrity is ensured using this paradigm. Subjects and objects are frequently divided into several security levels in such systems. Depending on his security level or access level, a person can only access items at specific levels.

This is another type of information security model which was used to ensure the integrity of information. In these models there are two main parts one subjects and the other objects which are segregated into different security levels. The subject can access only objects at specific level determined by his access level.

The below Fig.4 is explaining the structural aspects of the Biba model.

SIMPLE INTEGRITY RULE: In this the users (or) subjects can only READ the data on the same level of access and the upper level of access but can’t read data to the lower level of access. This rule is called NO READ DOWN.

STAR INTEGRITY RULE: In this the users (or) subjects can only WRITE the data on the same level of access and the lower level of access but can’t write data to the upper level of access. This rule is called NO WRITE UP.



1. *Biba Model*

Biba model is using these rules to improve the INTEGRITY of the data that is been shared. Information is validated using integrity. It determines whether or not the information is in the proper format. Additionally, it confirms that the information is accurate and true for the intended purpose. Integrity guarantees that the information sent to the recipient is the same information sent to the originator.

Biba model is using these rules to improve theintegrity of the data that is been shared. The **integrity** implies that the data is been validated. It gives an authentication on whether the data available in the network is in correct format or not. It also validates data whether it is true and correct to its original source of data. Integrity makes sure that the data presented by the publisher is been received in the same way to the receiver.

Biba model is using these rules to improve theintegrity of the data that is been shared. The **integrity** implies that the data is been validated. It gives an authentication on whether the data available in the network is in correct format or not. It also validates data whether it is true and correct to its original source of data. Integrity makes sure that the data presented by the publisher is been received in the same way to the receiver.

Simple integrity rule: In this the users (or) subjects can only **read** the data on the same level of access and the upper level of access but can’t read data to the lower level of access. This rule is called **no read down**.

1. **Clark Wilson security model:**

The protection of information integrity from hostile data manipulation efforts is the cornerstone of the Clark-Wilson security paradigm. The security paradigm emphasises that only authorised users should be able to create and modify the data, and that the system should maintain consistency between internal and external data. No alterations should be possible by unauthorised users.

For the Clark-Wilson model, a transaction must be properly constituted. Only lawful operations may be carried out thanks to a security mechanism that guarantees transactions are well-formed. assures that the internal data is reliable and consistent with what it means in practice (Blake).

The Clark-Wilson model also heavily incorporates the notions of separation of responsibilities. For the concept to be implemented effectively, the implementer, auditor, and certifier must all be distinct individuals (Blake).

By 1987, Wilson and Clark were two of many who had discovered that academic research on access control models prioritised data confidentiality above data integrity (i.e., the work showed higher concern for unauthorised observation than for unauthorised alteration). according to an article written by Sonya Blake and published on soft panorama. As a result, they made an effort to correct what they believed to be a military perspective that significantly varied from a commercial one. What they believed to be a military viewpoint, however, was not widely held inside the military.

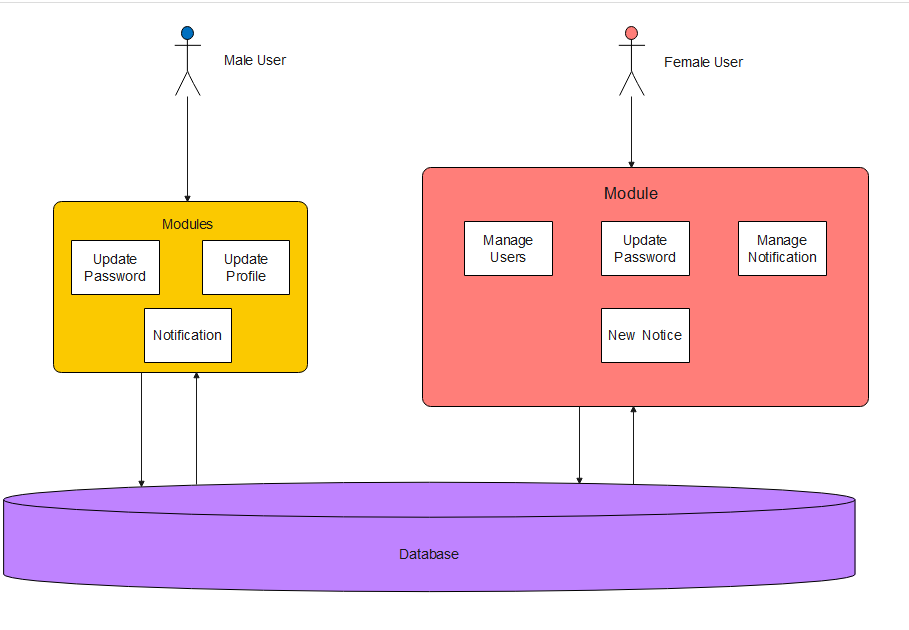
As you can understand, there are situations in which data integrity may be of the utmost importance and regarded as even more crucial than data secrecy. This might occur in a variety of military contexts where the integrity of assault instructions for technical, atomic, and biological warfare must be 100% guaranteed.

**Availability:**

This implies that users should always be able to access the network. This applies to both the system and the data. Network administrators should maintain hardware, carry out routine updates, and steer clear of bottlenecks to guarantee network availability. A network may become useless as a result of attacks like DoS or DDoS (Distributed Denial of Service), which manipulate the network's resources. Users who depend on the network as a business tool experience significant negative effect.

1. **Modules:**

The project is creating a network with the integration of Information security policies like Bell-LaPadula model and BIBA model for the different features of users. The data of the users are been stored in a private and personal database for securing their details in two different tables naming Female User’s and Male User’s.



1. *Architecture Diagram*

The above diagram Fig.5 is the explaining of the multiple modules of the applications.

The Male users are given the options (or) features of updating their profiles and viewing the notices that are been posted into the network and can create a relation with the members of the network by the option friends.

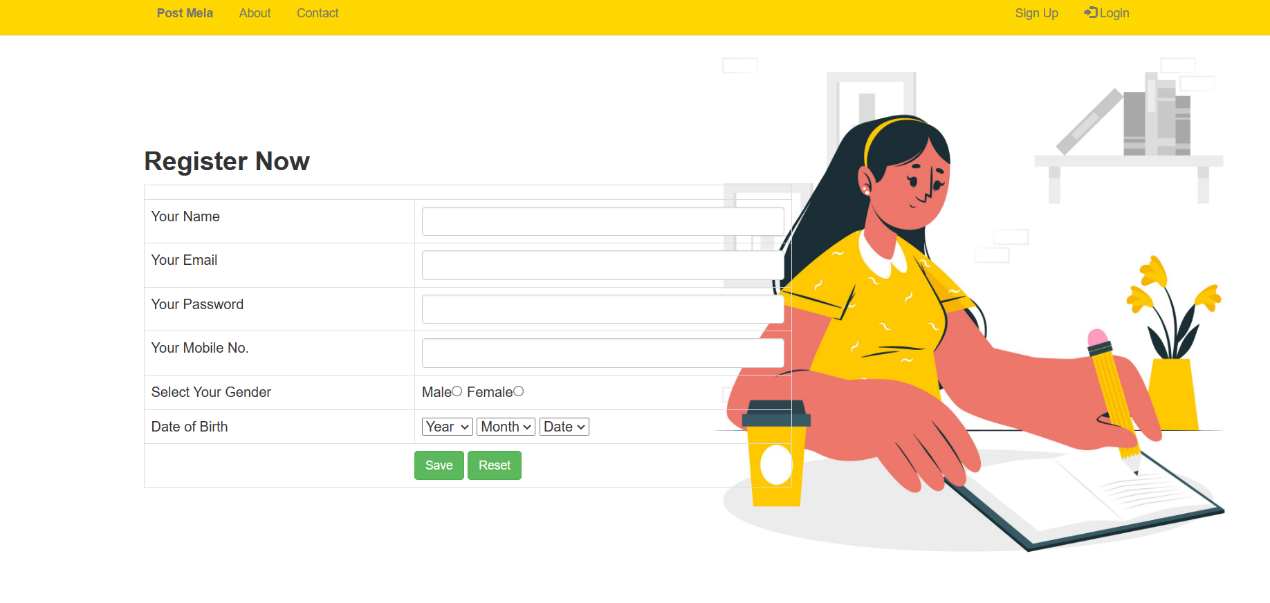
The Female users are having the features like managing users, updating their profile, Managing Notices and creating a new notice. Here the application is incorporating the Bell-LaPadula model into the network where the female users are in the superior authority in the process of creating a post and editing it (or) deleting it permanently from the network is their hands.

1. **Implementation:**

A website with complex combination of webpages to create a secure network to interact with individuals who are willing to help the needed by sharing the needful. We are creating the one page for the Registration process.

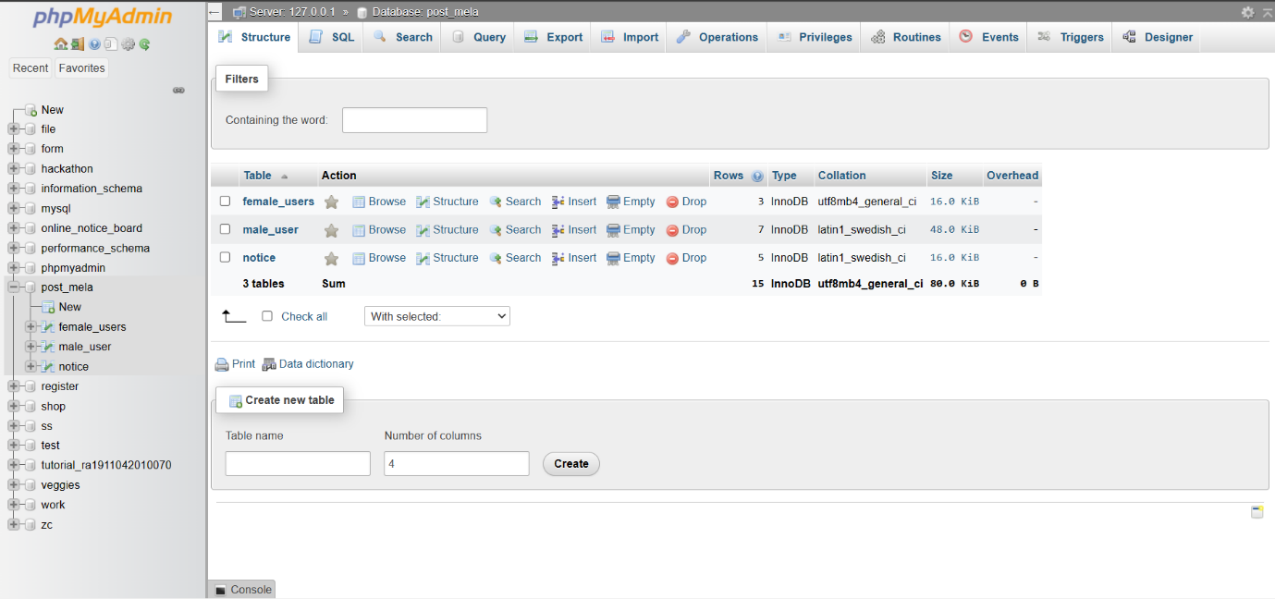
**3.5.1 Registration Page:**

One has to get registered in this page to login into their personalized account to view the posts (or) create a post. This is containing the attributes like User’s Name, User’s Email, User’s password, User’s Mobile number, User’s gender, User’s DOB which can be viewed in Fig.6.



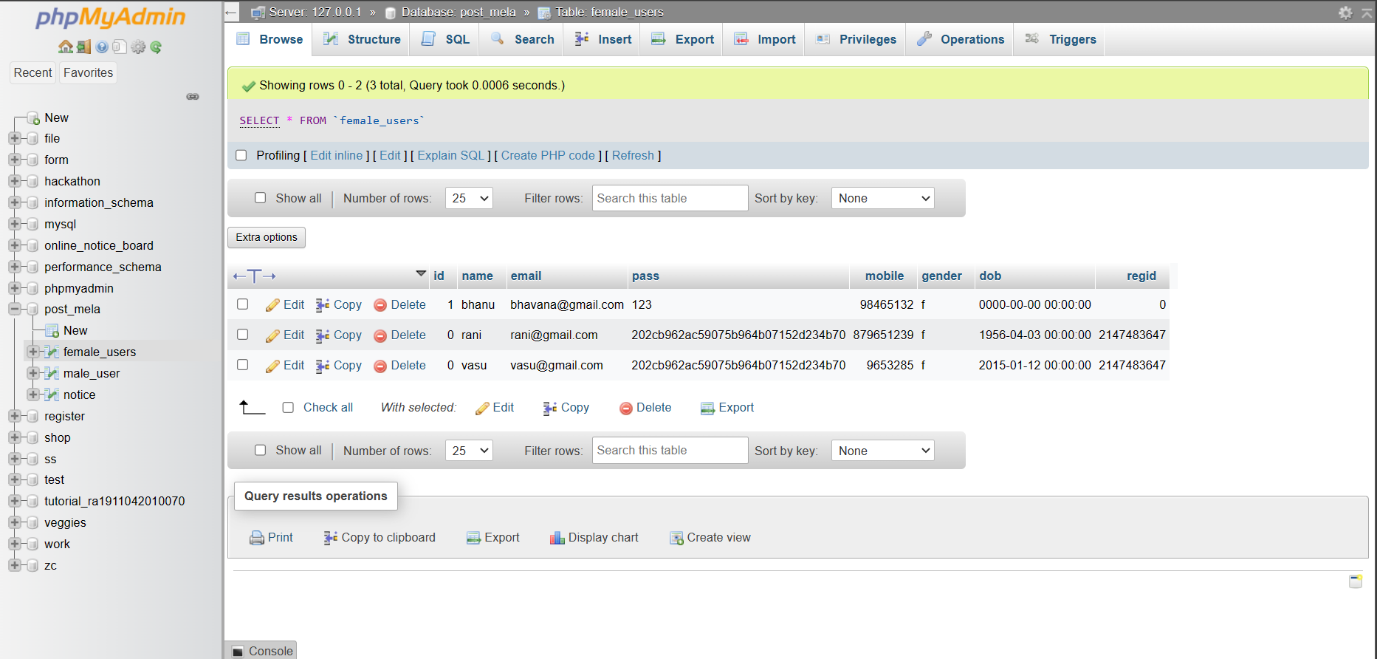
1. *Register Page*

The data that is entered by the users is been stored into the data base and segregated into two different tables according to the gender of the user to give a specific hierarchy to the users according to the gender of the user as we can view in the Fig.8 and Fig.9.

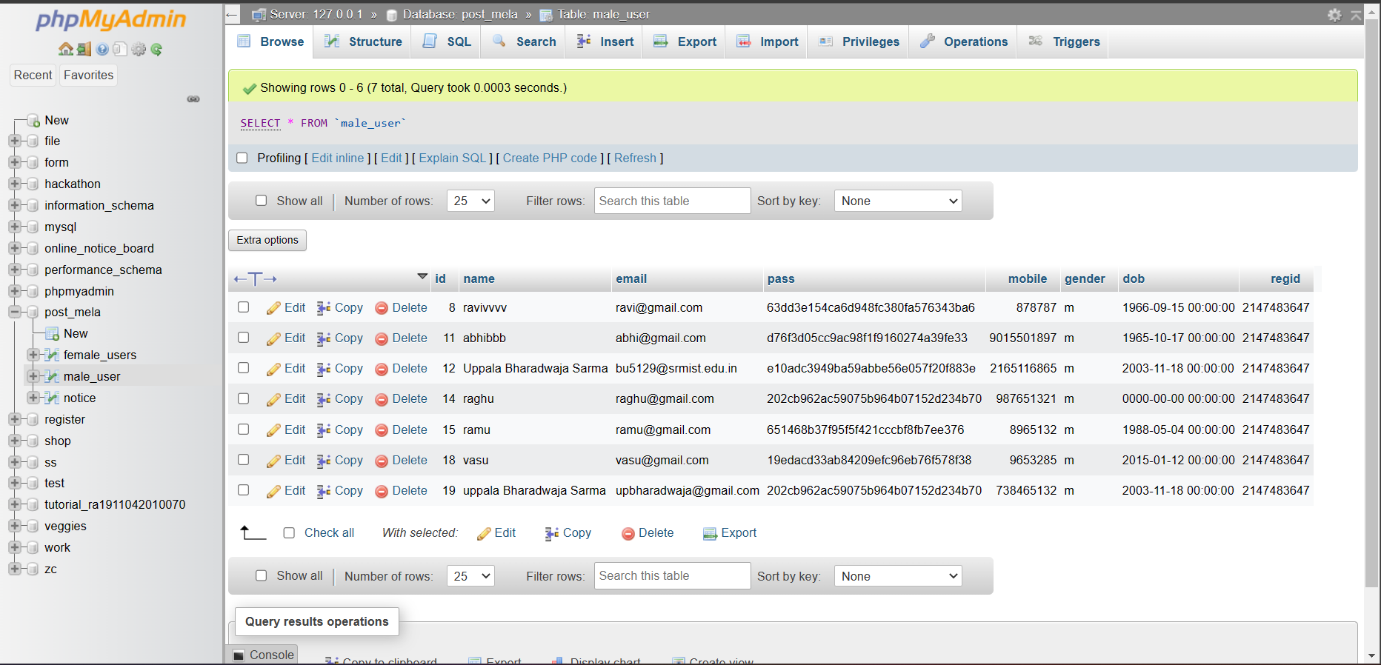


1. *Complete Database of the Project*

The above Fig.7 is the complete database of the application. The few of the main features of the form is that the user’s password can’t be viewed even by the developer to get the better of security aspect of the users and all the details filled by the users is visible to whoever can access the data base.



1. *Female user’s table*

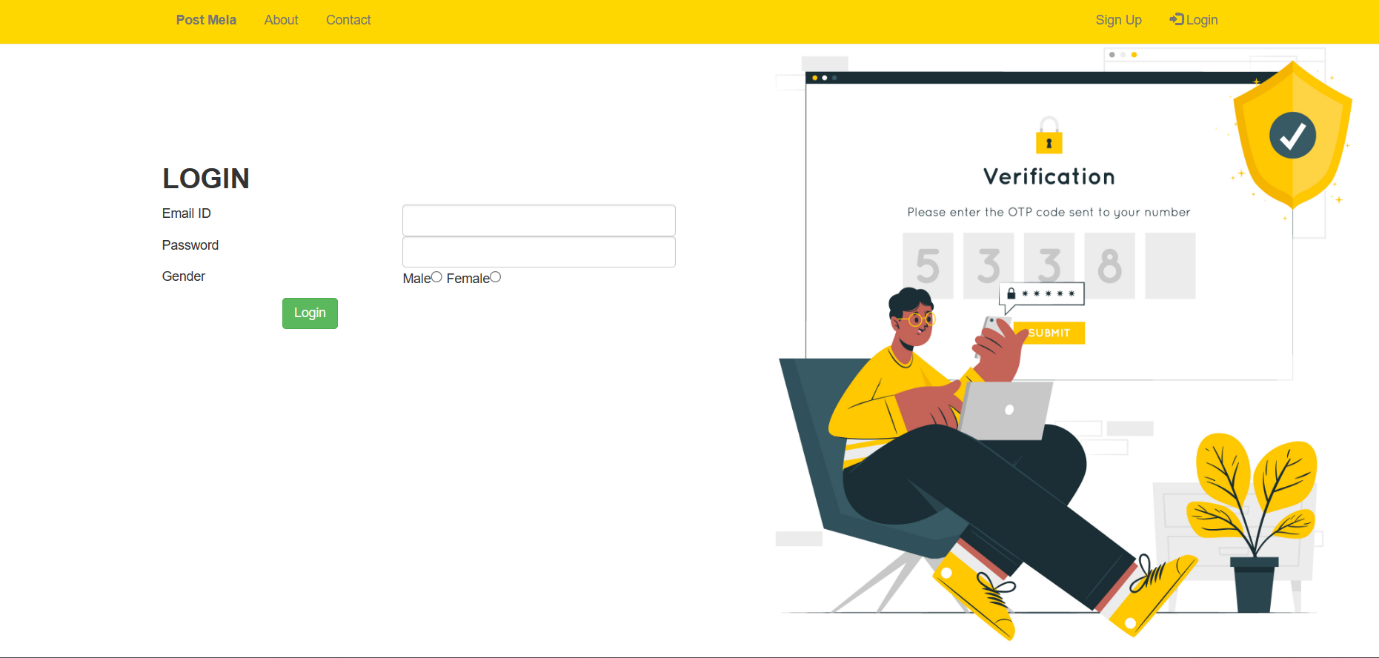


1. *Male user’s table*

**3.5.2 Login Page:**

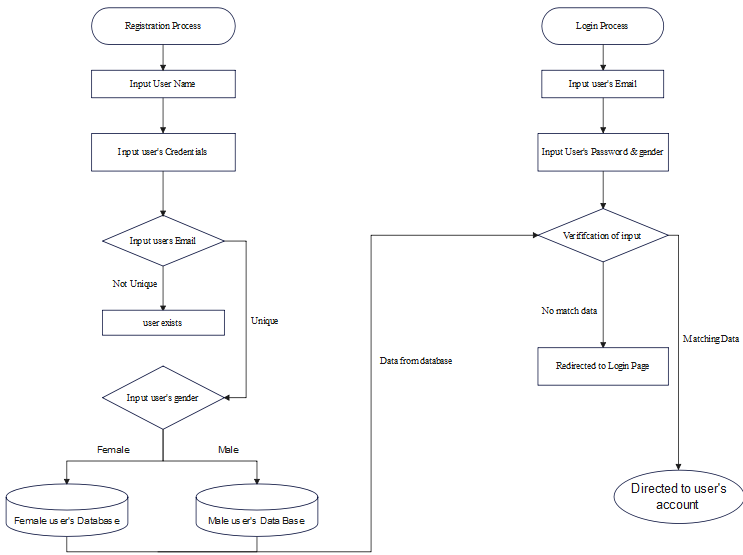
Here the page is used for logging into the personal account to view their posts and post their new posts into the network. This is using the user’s email id and the user’s password and their gender to login into their account.

The login credentials are been verified with the database of the male users and female users while logging into user’s account as shown in the Fig.10. Once the user longs into his /her account then they give few features to use the application and communicate with the network of users.



1. *Login Page*

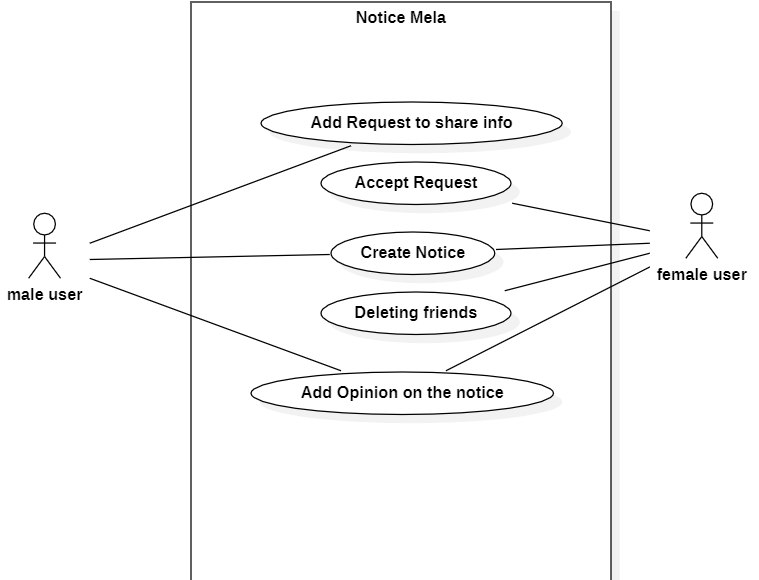
As the Fig.11 show this is the flow of the users through the application and how the data is been navigating between the backend and frontend i.e., from the applications to the database and vice versa.



1. *Flow Diagram*

The first step is as registering themselves into the network where their credentials will be authenticated and be compared with the existing database once if the data is unique and verified the user gets registered themselves into the network. And as the user gets registered the data is stored in the different tables of the same database on the aspects of the gender of the user.

The latter part of the network is logging into the network using their credentials which are been checked with the database if the match is found then the users are navigated to their personal account space, where they are given the following features on the basis of the gender.

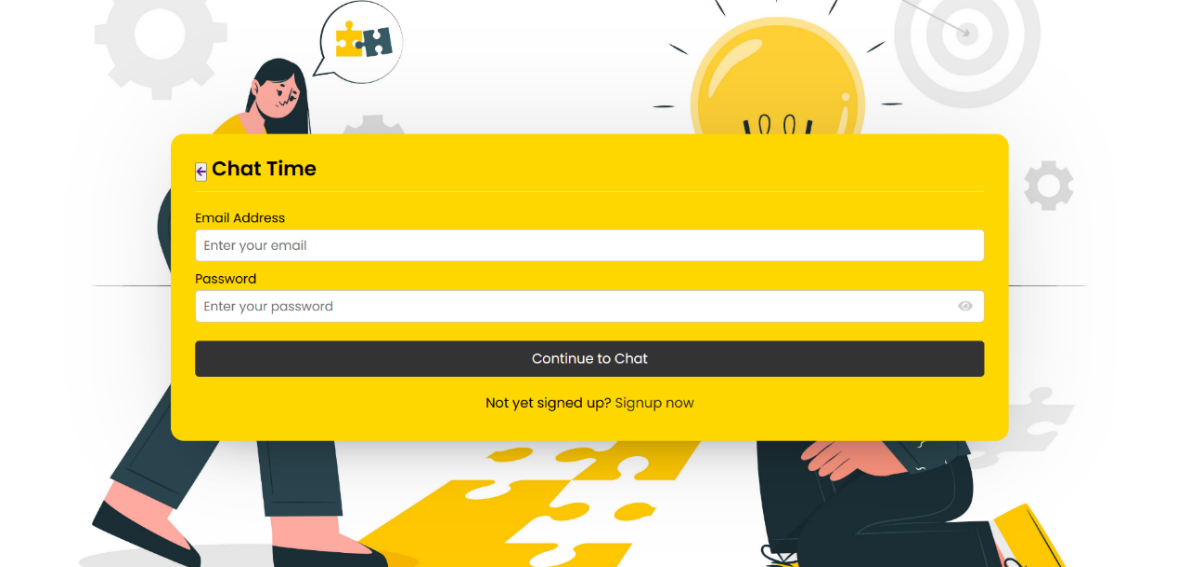


1. *Activity Diagram*

The above Fig.12 activity diagram is giving a crystal-clear picture over the feature that are accessible for both female users and male users. Like creating notice, adding friend request, Accepting request, etc.…

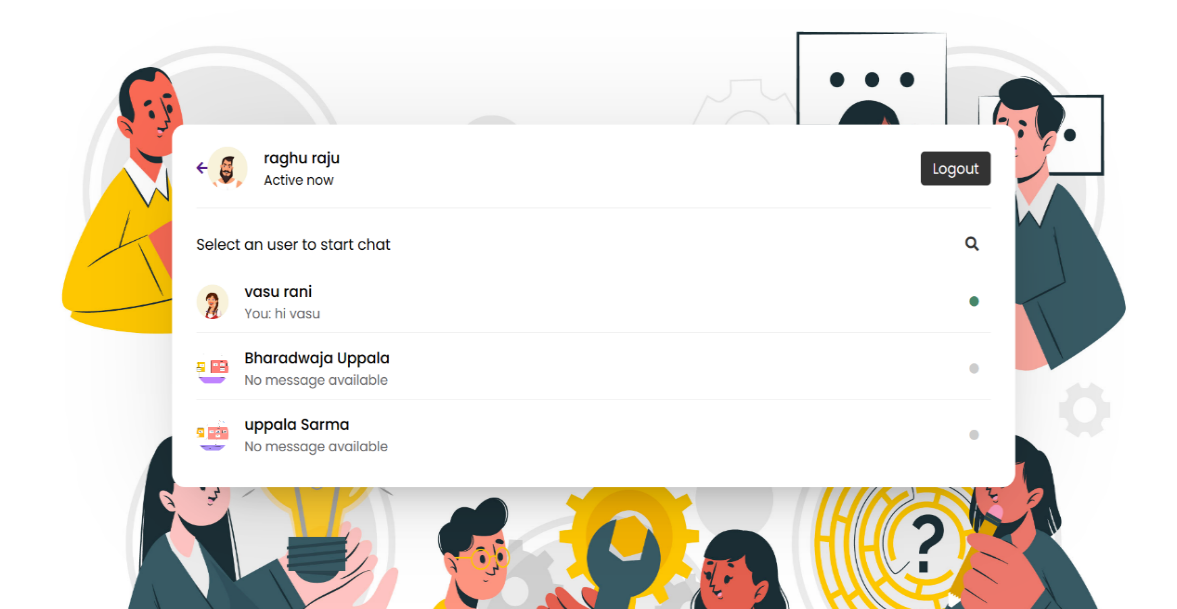
**3.5.3 Chatting:**

Once the users get into their account, they can search their friends and can start a communication with them as shown in the Fig.13. As the user’s choose the option of “friends” user’s are asked to login once again.



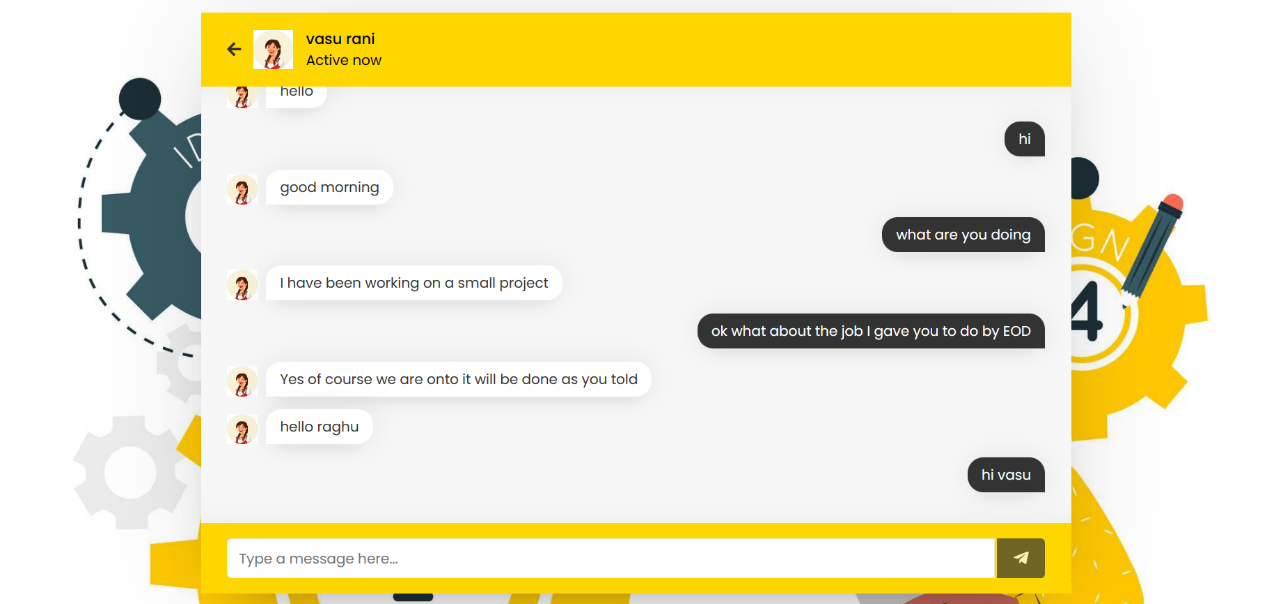
1. *Chat Login*

Then the users are able to view the friends over the screen and then find who is online and who isn’t online and then choose to chat with anyone as we can see in the Fig.15 and Fig.14 given below.



1. *Friends List*

Rather than sharing complete personal details or contact with random members of the network one can just establish a connection by creating a friend request and start a basic communication once they are ok of sharing their personal contact, they could any time.



1. *Chat Space*

The users are giving the users a feature to have a communication with each other which enhances the user’s experience of using the network. Once the user logins then he/she can view the number of user’s they can communicate with. They can chat with the users by using this feature of the network.

**CHAPTER 4**

**RESULTS AND DISCUSSION**

Information security is a critical aspect of any website, especially when it comes to handling sensitive user data. In today's world, where online privacy is becoming increasingly important, it is essential to have a strong security framework in place to safeguard user data. To ensure the security of our website, we have implemented various security measures and Information Security Policies. These measures include data encryption, multi-factor authentication, regular security audits, and user access controls.

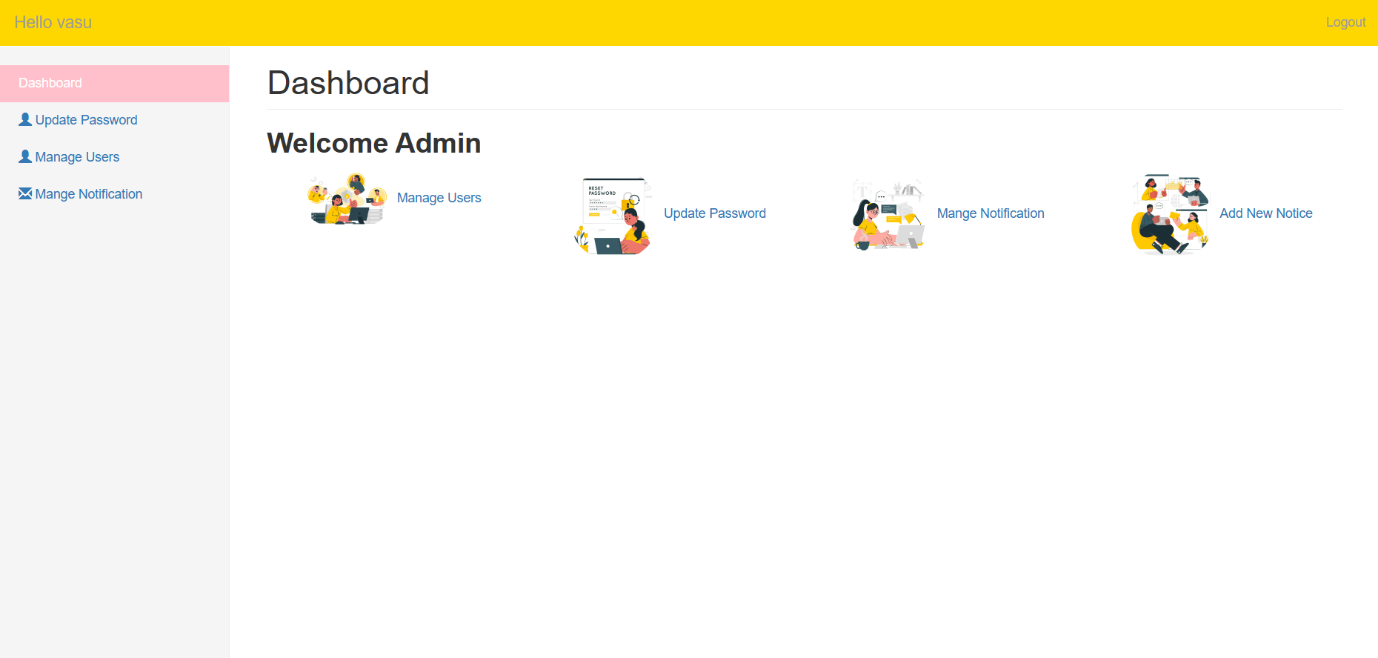
Data encryption is a crucial component of our security framework, ensuring that sensitive user information is protected from prying eyes. We use strong encryption algorithms to protect user data both in transit and at rest. This means that any information exchanged between our website and users is protected from interception and theft. We have also implemented multi-factor authentication to provide an extra layer of security for user accounts. This feature requires users to enter a unique code sent to their registered email or phone number, in addition to their password, to access their account. This ensures that only authorized users can access their accounts, even if their password is compromised.

**4.1 Female Users:**

Once logging into the account the female users are able to view their DASHBOARD with the options like **Manage Users, Update Password, Manage Notification, Add New Notice and chat** are the features that are available for the users as in the Fig.16.

By this they view the members of the network, they can create (or) edit (or) delete the posts they have posted into the network and can choose the option to share the information to a particular individual or not is completely in their hands.

***But they can’t edit the comments of the male users (or) any other user but can only view them.* This is where the Information security policies are been incorporated into the application this is said *Bella-Lapadula model.***



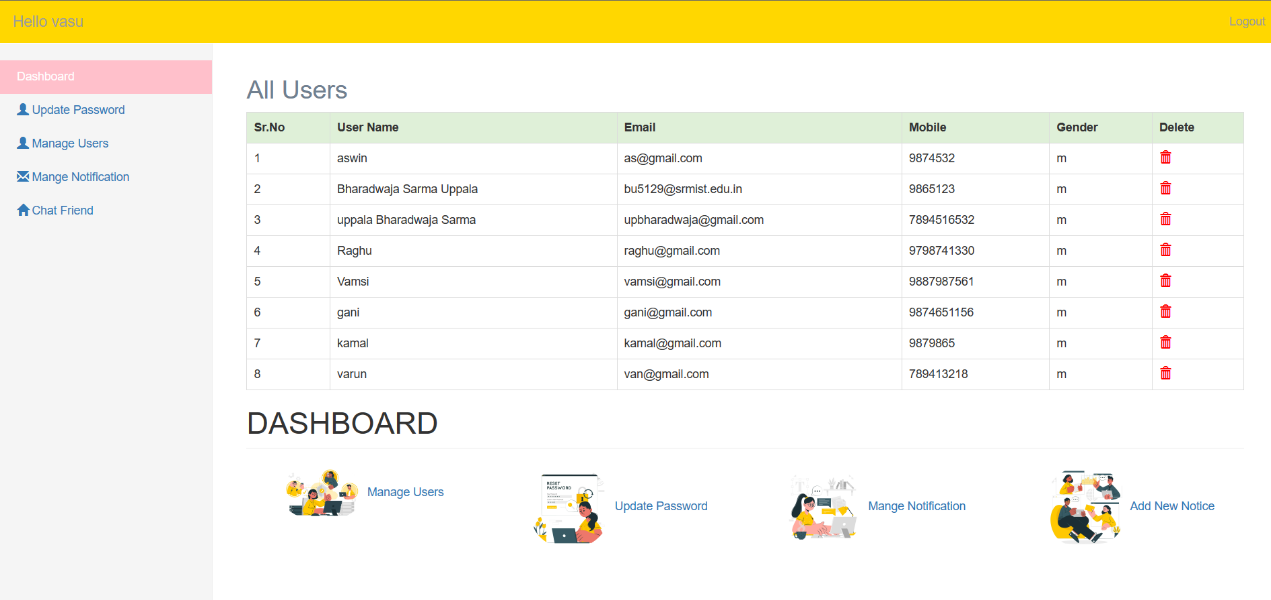
1. *Female User’s Dashboard*

**4.1 (1) Update Password:**

They can update their passwords at this page. The Old password is been compared with the data base and if it matches then password of the user can be changed.

**4.1 (2) All Users:**

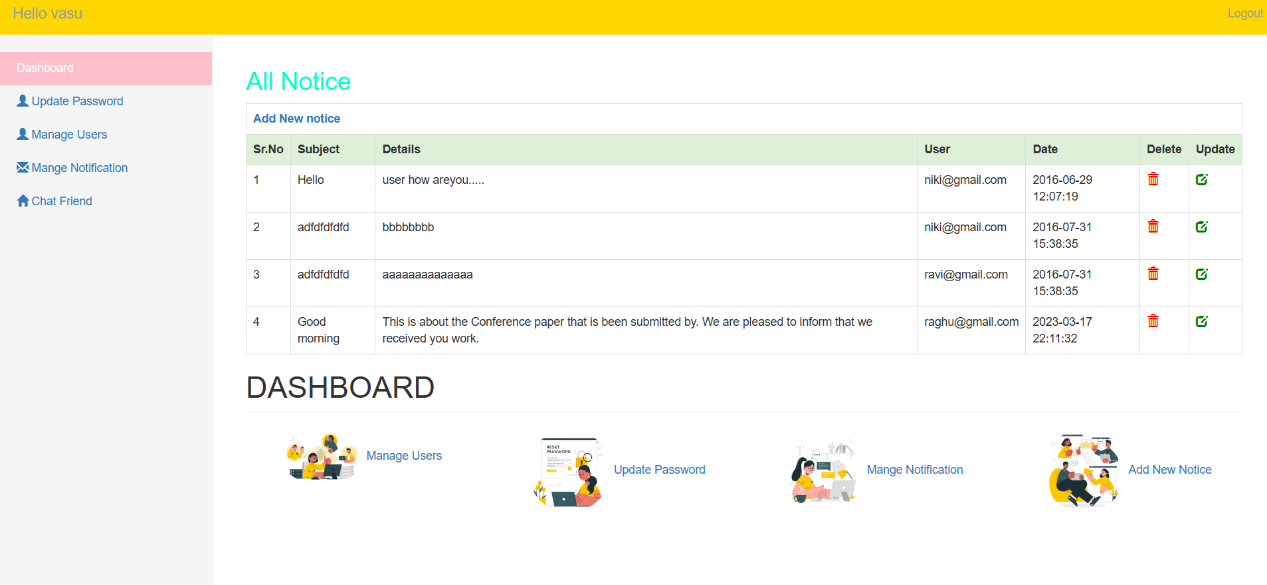
Here the female users can view all the members of the network and can choose to delete any user of their choice from their network of members.



1. *All user’s page*

**4.1 (3) All Notices:**

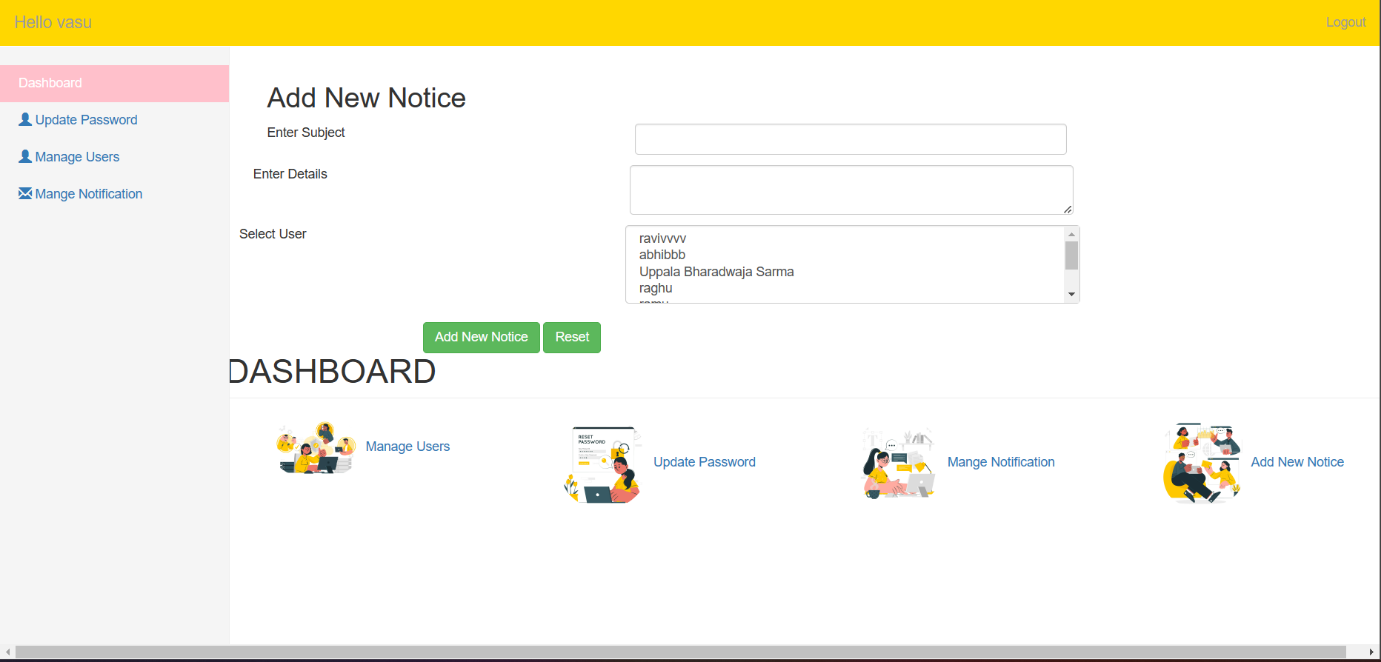
As in the Fig.18 the user can delete (or) Update their post to the members of the network at any point of time which gives them complete control over their posts into the network.



1. *Notice Page*

**4.1 (4) Add New Notice:**

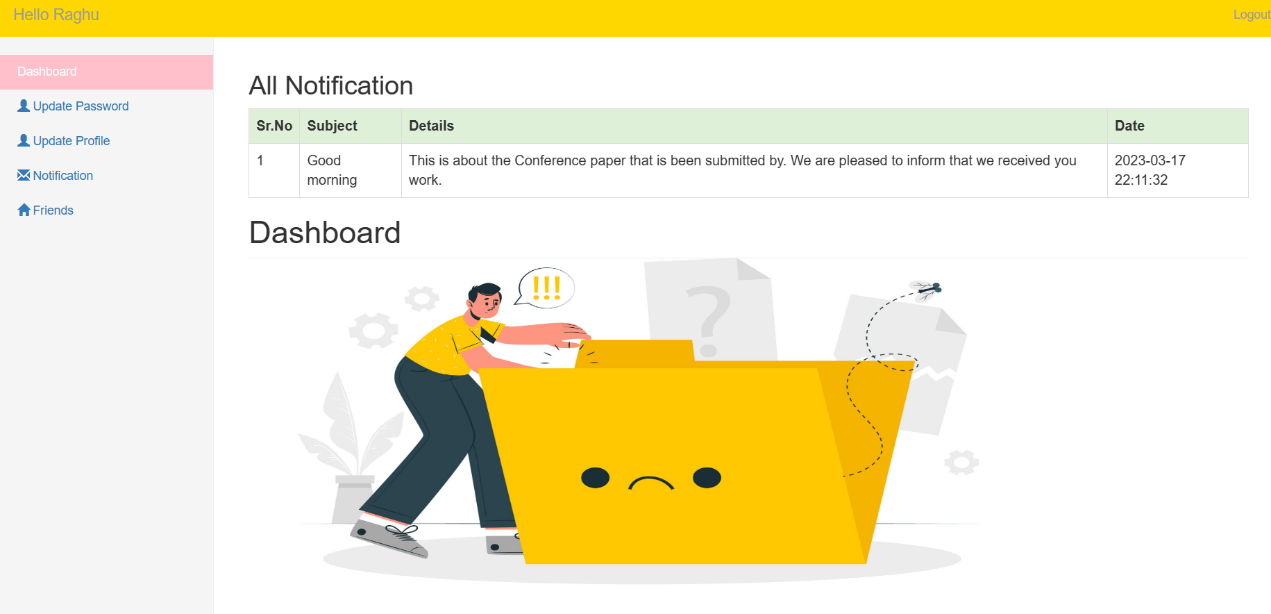
Here as we can view in the Fig.19 female users can create a new notice and upload it into the members of the network.



1. *Create a Notice Page*

**4.2 Male Users:**

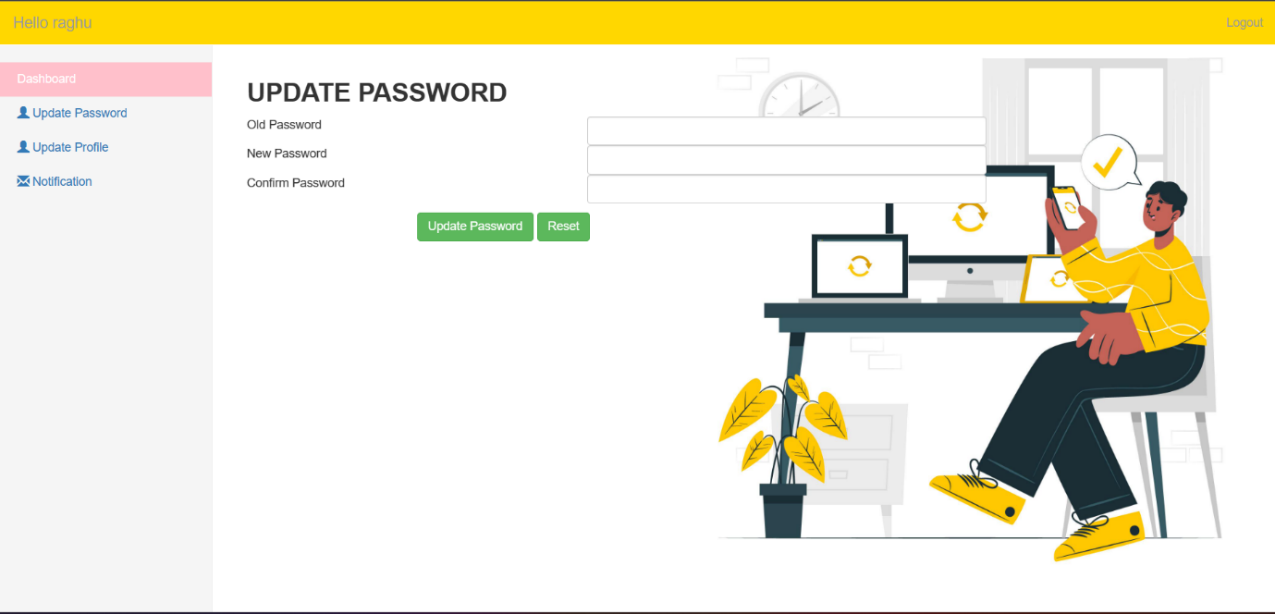
If a user is logging using the credentials and selecting the gender as male, then they are navigated into a new page dash board where they can view all the notices that they receive from the members of the network.



1. *Male user’s Dashboard*

**4.2 (1) Update Password:**

At this page is used for the same purpose for male and female users, to update their passwords for logging in their accounts. The old password is been verified with the data base from the registration process.



1. *Password Update Page*

**4.2 (2) Update Profile:**

This page is used for the updation of the user’s information like user’s name, user’s mail id, user’s mobile number, user’s gender and user’s DOB as shown in the Fig.22.

1. *Profile Update Page*

The changes made in this page is been modified even in the database as they save the dat is been changed.

Her the Male Users can only view the posts and add a comment to the posts that are been posted can only view them but can’t edit the data that they are sent. **This is the phase where the second phase of the security policy Bell-LaPadulla is been kept into application.**

User access controls are another important aspect of our security framework. We have implemented strict access controls to ensure that only authorized users can access sensitive data. This includes limiting access to user data based on user roles and implementing strict password policies.

Apart from implementing strong security measures, we have also built a social media platform for connecting job seekers with employers. This platform provides a better space for job seekers to search for job opportunities, while also providing employers with a way to find the best candidates for their vacancies.

The next part where we are combining the Information security model into the network is in the feature of the male users can only view the posts that are been posted into the network but are not allowed to edit the content that is available in the post, but could comment over it, this is called the Biba model. But can edit it once they get the access from author of the post.

This is creating a more reliable and secure network where one asks for help without fearing of fake users and hijacking over the network for getting the members personal information. Once the members of the network feel more secured and improve their trust over the network the CEI of the network will also improve gradually.

Overall, we believe that our security framework is robust and effective, providing users with the confidence to use our website and share their sensitive information with us. We remain committed to continually improving our security measures to ensure that our website remains a safe and secure platform for job seekers and employers.

**CHAPTER 5**

**CONCLUSION AND FUTURE ENHANCEMENT**

1. **Conclusion:**

This application is mainly trying to introduce a new way of creating a network to have a more secure, accessible and reliable network by using Information Security methodologies incorporated into the process of creating the network and establishing it. Then tried to use it to improve the way the users interact in the network and build it for a better communal environment which encourages users to be a part and grow themselves. The effects of good network will improve the way one can create communal energy to achieve a specific goal, encourage users for initiating anything that they thought of (or) can be a part of it. And is also trying to take a leap onto find the way to integrate Information Security into the network to develop a more secure environment. Where we can develop a more secure and dependable network, more users could be encouraged to be a part of the network in the present times, as the present scenario of new social networks being developed every day and available in the internet. This network is trying to provide an insight on how the integration of information security models impact the working of the social network in real time in various aspects. Trying to get a foresight on how the impact of community energy initiative (CEI) to build systems which are effective in indulging members of it.

There are many mays for solving and finding solutions for every new issue that are raising or could develop in the coming futures. Nevertheless, the existing technology’s reliability and usability for regular users is seems to be a damaged in the process of establishing a better and more secure controls. In the end, all the protocols that are used for analyzing have failed to find or estimate the relation between more security of the network precautions and network performance.

1. **Future Enhancement:**

In the future the network can improve more in the aspect of the security of the user. This one is a very basic template of registration. The inclusion of the real time verification of user’s email id by OTP generation could be next step in the process of development. Later to this we can create more sophisticated process where when user registers themselves the photo, they use for the *DP* can be compared with the real time user’s face using facial recognition from stopping fake users in the network where male users can be controlled from creating fake female accounts in the network.

In the future, it would be desirable to have enhancements made to the architecture as well as reductions made to all of the barriers that prevent the system from being highly efficient. This would result in faster storage and retrieval times. If our approach were chosen in place of the more traditional method of document verification and storage, it would imply that an extremely large amount of data would need to be saved in google doc.. We would need to highly decompress the documents while keeping in mind that the quality should not be compromised or lost in the process. Storing the documents in their original size would not be an ideal situation to be in. It would also result in a significant increase in the amount of traffic that goes to the website, and our website ought to be able to cope with such a significant increase in the load. Developing a graphical user interface (GUI) that is more accessible to people of all ages and backgrounds by making its operations simpler and improving its color palette, typeface, and transitions. Another enhancement that is planned for the application in the near future, the distribution of APIs for usage by the general public for development / learning purposes.

In the future we are looking to improve the facial recognition and more secure registration pages to which helps the users to trust the website to use and express their ideas and opinions on the posted ideas in our platform.

**REFERENCES**

1. Zhiyong Zhang, Brij B. Gupta: “Social media security and trustworthiness: Overview and new direction”, [Volume 86](https://www.sciencedirect.com/journal/future-generation-computer-systems/vol/86/suppl/C), September 2018, Pages 914-925
2. C. Sushama, M. Sunil Kumar, P. Neelima: “Privacy and security issues in the future: A social media”,Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 7, 2022, pp. 4062-4074
3. Victor Chang, Karl Hall, Qianwen Ariel Xu, Le Minh Thao Doan, Zhi Wang: “A social network analysis of two networks: Adolescent school network and Bitcoin trader network”, *Decision Analytics Journal*, Volume 3, June 2022, 100065
4. Zhi-Jin Zhonga, Ruiyao Jiang, Sini Sua, Shujin Lina: “Do men and women differ in the capability of weaving online social networks: A perspective of gender Stereotype activation”, [Volume 8](https://www.sciencedirect.com/journal/telematics-and-informatics-reports/vol/8/suppl/C), December 2022, 100018
5. Antti J. Tanskanen: “Deep reinforced learning enables solving rich discrete-choice life cycle models to analyze social security reforms”, *Social Science & Humanities Open,* [Volume 5, Issue 1](https://www.sciencedirect.com/journal/social-sciences-and-humanities-open/vol/5/issue/1), 2022, 100263
6. Yingjie Zenga: “AI Empowers Security Threats and Strategies for Cyber Attacks”, *Procedia Computer Science,* [Volume 208](https://www.sciencedirect.com/journal/procedia-computer-science/vol/208/suppl/C), 2022, Pages 170-175
7. Kaouthar Chetiouia \*, Birom Baha, Abderrahim Ouali Alamia, Ayoub Bahnasseb: “Overview of Social Engineering Attacks on Social Networks”, *Procedia Computer Science,* [Volume 198](https://www.sciencedirect.com/journal/procedia-computer-science/vol/198/suppl/C), 2022, Pages 656-661
8. Tanja Grassegger, Dietmar Nedbal: “The Role of Employees’ Information Security Awareness on the Intention to Resist Social Engineering”, *Procedia Computer Science,* [Volume 181](https://www.sciencedirect.com/journal/procedia-computer-science/vol/181/suppl/C), 2021, Pages 59-66
9. Seyyed Mohammad Safi, Ali Movaghar, Mohammad Ghorbani: “Privacy protection scheme for mobile social network”, *Journal of King Saud University - Computer and Information Sciences*, Volume 34, Issue 7, July 2022, Pages 4062-4074
10. F. Goedkoop \*, J. Dijkstra, A. Flache: “A social network perspective on involvement in community energy initiatives: The role of direct and extended social ties to initiators”, *Journal Energy Policy*, Volume 171, 113260, Pages 15
11. HaiderMehrajaD.JayadevappabSulaima Lebbe AbdulHaleem c Rehana Parveend Abhishek Maddurie Maruthi Rohit Ayyagarif Dharmesh Dhabliyag: “Protection motivation theory using multi-factor authentication for providing security over social networking sites”, *Pattern Recognition Letters*, Volume 152, December 2021, Pages 218-224
12. David Tayouri: “The human factor in the social media security –combining education and technology to reduce social engineering risks and damages”, *Procedia Manufacturing*, Volume 3, 2015, Pages 1096-1100
13. Social network security: “Issues, challenges, threats, and solutions”, *Information Sciences*, Volume 421, December 2017, Pages 43-69
14. David W Chadwick: “On the Modelling of Bell-LaPadula Security Policies Using RBAC”, DOI: 10.1109/WETICE.2008.34
15. Stephen D. Gantz, Daniel R. Philpott: “Federal Information Security Fundamentals”, *FISMA and the Risk Management Framework,* The New Practice of Federal Cyber Security,2013, Pages 23-52
16. G. Zhao and D. W. Chadwick, "On the Modeling of Bell-LaPadula Security Policies Using RBAC," 2008 IEEE 17th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, Rome, Italy, 2008, pp. 257-262, doi: 10.1109/WETICE.2008.34.

**APPENDIX 1**

**FRONT END:**

A website for uploading documents that we want to put on the block so that a user can see and interact with them directly is created using HTML, CSS, and JS in front-end web development, which is client-side programming. When users open this website, the designers want to make sure that the content is presented in an accessible and pertinent manner.

HTML:

Hyper-text markup language, is the language that is been used for generating online pages and web applications. A web browser translates documents that are mostly written in HTML. There can be static or dynamic web pages. HTML is capable of producing totally static web pages. As a result, HTML is a language of markup which is used for creating visually likeable web pages that display in a pleasing manner to a web browser. There are many HTML tags, which make up to a HTML document, and each one of them have their own content.

CSS:

The abbreviation CSS stands for cascading style sheets. It is a style sheet language that specifies how markup-language texts should be set up and look. It usually works alongside HTML to change the visual appearance of websites and user interfaces. The majority of websites employ a combination of HTML, CSS and JavaScript to construct user interfaces for web applications and many mobile apps.

The three main advantages of CSS are as follows:

1) Add more attributes.

CSS provides more precise features than plain HTML to define the look and feel of the website.

JavaScript is a scripting or programming language that makes it possible to implement complex features on web pages., and so forth — JavaScript is almost certainly used. The conventional web technology layer cake has it as the third tier. With the help of the scripting language JavaScript, you can very much do anything, including dynamically update material, manage multimedia, and animate graphics.

JavaScript was created for:

- Speed: a web browser's native language code execution is quicker than server-side code execution.

- Dynamic pages: Before the advent of JavaScript, interactive pages were not conceivable.

- Less memory usage: by running the code in the browser, server space is freed up, which lowers costs.

- Making responsive user interfaces: Nearly all social media user interfaces employ JavaScript.

- Independently reloading particular sections of the page: JavaScript is in charge of the search suggestion boxes that pop up in Google's search bar.

- Responsive content: JavaScript changes the size of the content on the page in accordance with the size of your browser window.

• Putting a lot of effort into adding features that will help female users feel more secure and inspired to share their ideas.

• The goal of our project is to develop a website that will enable women to participate in the business world with their ideas and company plans by giving them a safe space to express their ideas and as much support as possible.

• They might reach a wider audience on this website; therefore, this is even intended to present their sales pitch.

• In order to prevent fraudulent profiles and anonymous users, we are developing a registration process that incorporates facial recognition.

• Women users will be in a position to take the initiative in the network and protect users' privacy.

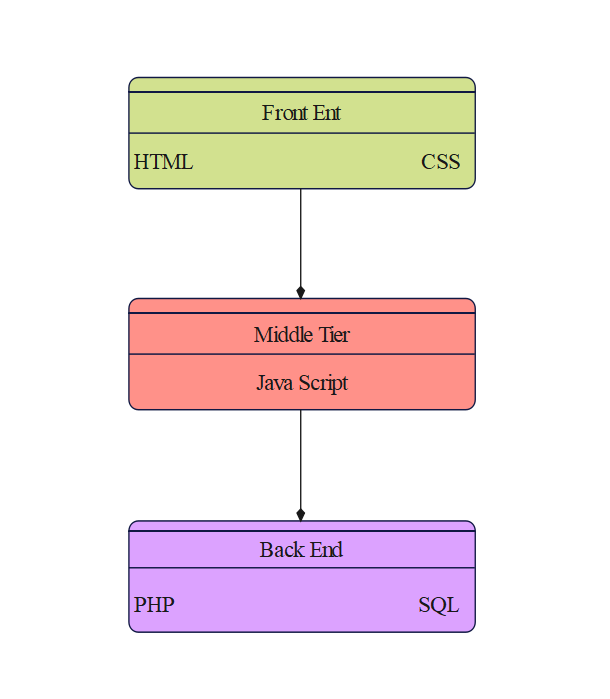
• When asking users to provide a profile picture for their accounts before comparing that picture to a real-time facial recognition system.

**Middle Tier**

In most situations, the majority of the application logic is housed in the middle tier which supposed to be one of the three-tier web database systems. The client-side tier displays data to the user and requests data from them, whilst the database layer stores and retrieves data. The middle layer controls how data is displayed to users and how user input is transformed into database queries to read or write data. as well as the majority of the remaining tasks that connect the other tiers. The HTTP protocol also includes state management. The middle-tier application logic integrates the database management system with the web. NodeJS: Despite the fact that it is used for programming on the server and is commonly deployed for non-blocking, event-driven servers such as regular web pages and back-end API applications, it was designed with architectures based on push technology in mind.

**BACK END**

Back-end development is the term used to describe server-side development. Databases, programming, and website design are the main topics. It explains what happens in the background when a user completes any action on a website. Making an online purchase or signing into an account could be examples. Back-end creates the code that connects browsers to database data. The portions of a computer application or program's code known as the "back end" are those that enable it to run but are inaccessible to users. The back end of the computer system is where the majority of data and operating syntax are kept and accessed. Programming languages often make up one or more portions of the code.



1. *Full-Stack*

The handling and manipulation of user data in databases and tables is then taken care of in the backend using SQL. The application is then kept up to date by PHP for data collection and application access from the database. As the Fig.24 is giving the structure of the full-stack development.

**IMPLEMENTATION OF SECURITY**

A username or email field, a password field, and a bottom for logging in are the typical components of a login form. The username and password are typically the two main components of the login procedure. The credentials are checked in the database and promoted appropriately when a user enters their username and password in the appropriate fields and clicks the login button. The user can log in if the credential combination is right; otherwise, they cannot. We can also employ two-factor authentication, which requires the user to complete an additional verification step after entering their username and password correctly.

OTP (One Time Password), which is sent via email or phone, or responding to security questions, could be another step. In essence, a login form is a record form with disabled insert, update, and delete features.

In this instance, we are integrating facial recognition technology into the registration and login sites. Therefore, the user is not permitted to use fictitious profile images when registering oneself. The security of anonymous users is being improved by this.

In this regard, female users are given preference, except that they can choose to share their ideas first and keep their personal information hidden for as long as they like. At any time, they have the ability to post and change content. Even the decision of to whom they wish to post the material is offered to them. They are also able to add and remove buddies.

Male users have access to the content, can comment on it, and can add female users as friends. If they agree, they can give them the material privately so that no one else can comment on it in public.

**Role Based Access Control:**

The role based access control model is been widely implemented as natural model as it is very much suitable in most case scenarios. The results of the applications built on this model are growing very rapidly in commercial and educational institutions.

The function *Check Access* is used for authorizing decisionmade by the system is giving the users different roles in the network on the bases of the gender of the user *ex: female users are given role of higher level and male users are given a lower level.*

**APPENDIX 2**

**Source Code:**

**Index:**

<?php

$conn=mysqli\_connect("localhost","root","","post\_mela");

session\_start();

?>

<html>

<head>

<title>Post Mela</title>

<link rel="stylesheet" href="css/bootstrap.css"/>

<script src="js/jquery\_library.js"></script>

<script src="js/bootstrap.min.js"></script>

</head>

<body>

<nav class="navbar navbar-default navbar-fixed-top" style="background:yellow">

<div class="container">

<ul class="nav navbar-nav navbar-left">

<li><a href="index.php"><strong>Post Mela</strong></a></li>

<li><a href="index.php?option=about"></span> About</a></li>

<li><a href="index.php?option=contact"></span>Contact</a></li>

</ul>

<ul class="nav navbar-nav navbar-right">

<li><a href="index.php?option=New\_user"></span> Sign Up</a></li>

<li><a href="index.php?option=login"><span class="glyphicon glyphicon-log-in"></span> Login</a></li>

</ul>

</div>

</nav>

<br>

<br>

<br>

<br>

<br>

<br>

<br>

<br>

<div class="container">

<div class="row">

<!-- container -->

<div class="col-sm-8">

<?php

@$opt=$\_GET['option'];

if($opt!="")

{

if($opt=="about")

{

include('about.php');

}

else if($opt=="contact")

{

include('contact.php');

}

else if($opt=="New\_user")

{

include('registration.php');

}

else if($opt=="login")

{

include('login.php');

}

}

else

{

echo "<h1><b>'WELCOME TO OUR MELA'</b></h1>

<i> <b> Join us today and get connected. Register now to get each and every updates! </b></i>";

}

?>

</div>

<!-- container -->

<div class="col-sm-4">

<div class="panel panel-default">

<div class="panel-heading"><b>LATEST NOTICE</b></div>

<div class="panel-body">HI FROM ADMIN</div>

</div>

</div>

</div>

</div>

</div>

<br/><br/>

<br/><br/>

<br/>

</body>

</html>

**REGISTER:**

<?php

require('connection.php');

$conn = mysqli\_connect("localhost","root","","post\_mela");

extract($\_POST);

if(isset($save))

{

//check user alereay exists or not

$sql=mysqli\_query($conn,"select \* from male\_user where email='$e'");

$r=mysqli\_num\_rows($sql);

$g=$gen;

if($r==true)

{

$err= "<font color='red'>This user already exists</font>";

}

else if($g=="m"){

{

//dob

$dob=$yy."-".$mm."-".$dd;

//encrypt your password

$pass=md5($p);

$query="insert into male\_user values('','$n','$e','$pass','$mob','$gen','$dob',now())";

mysqli\_query($conn,$query);

}

$err="<font color='blue'>Registration successfull !!</font>";

}

$Sql=mysqli\_query($conn,"select \* from female\_users where email='$e'");

$s=mysqli\_num\_rows($Sql);

if($s==true)

{

$err= "<font color='red'>This user already exists</font>";

}

else if($g=="f"){

{

$dob=$yy."-".$mm."-".$dd;

//encrypt your password

$pass=md5($p);

$quer="insert into female\_users values('','$n','$e','$pass','$mob','$gen','$dob',now())";

mysqli\_query($conn,$quer);

}

$err="<font color='blue'>Registration successfull !!</font>";

}

}

?>

<script>

function ValidateGender(){

var gen=document.getElementByname("gen");

if(gen=='m'){

return true;

}

}

</script>

<h2><b>Register Now</b></h2>

<form method="post" enctype="multipart/form-data">

<table class="table table-bordered">

<Tr>

<Td colspan="2"><?php echo @$err;?></Td>

</Tr>

<tr>

<td>Your Name</td>

<Td><input type="text" class="form-control" name="n" required/></td>

</tr>

<tr>

<td>Your Email </td>

<Td><input type="email" class="form-control" name="e" required/></td>

</tr>

<tr>

<td>Your Password </td>

<Td><input type="password" class="form-control" name="p" required/></td>

</tr>

<tr>

<td>Your Mobile No. </td>

<Td><input class="form-control" type="number" name="mob" required/></td>

</tr>

<tr>

<td>Select Your Gender</td>

<td>

Male<input type="radio" name="gen" value="m" required/>

Female<input type="radio" name="gen" value="f"/>

</td>

</tr>

<tr>

<td>Date of Birth</td>

<Td>

<select name="yy" required>

<option value="">Year</option>

<?php

for($i=1950;$i<=2016;$i++)

{

echo "<option>".$i."</option>";

}

?>

</select>

<select name="mm" required>

<option value="">Month</option>

<?php

for($i=1;$i<=12;$i++)

{

echo "<option>".$i."</option>";

}

?>

</select>

<select name="dd" required>

<option value="">Date</option>

<?php

for($i=1;$i<=31;$i++)

{

echo "<option>".$i."</option>";

}

?>

</select>

</td>

</tr>

<tr>

<Td colspan="2" align="center">

<input type="submit" class="btn btn-success" value="Save" name="save"/>

<input type="reset" class="btn btn-success" value="Reset"/>

</td>

</tr>

</table>

</form>

</body>

</html>

**LOGIN:**

<?php

extract($\_POST);

$conn = mysqli\_connect("localhost","root","","post\_mela");

if(isset($save))

{

if($e=="" || $p=="")

{

$err="<font color='red'>fill all the fileds first</font>";

}

else

{

$pass=md5($p);

$g = $gender;

if($g=="m"){

$sql=mysqli\_query($conn,"select \* from male\_user where email='$e'and pass='$pass'");

$r=mysqli\_num\_rows($sql);

if($r==true){

$\_SESSION['user']=$e;

header('location:user\index.php');

}

else{

$err="<font color='red'>Invalid login details</font>";

}

}

if($g=="f"){

$Sql=mysqli\_query($conn,"select \* from female\_users where email='$e'and pass='$pass'");

$r=mysqli\_num\_rows($Sql);

if($r==true){

$\_SESSION['admin']=$e;

header('location:admin\index.php');

}

else{

$err="<font color='red'>Invalid login details</font>";

}

}

}

}

?>

<h2><b>LOGIN</B></h2>

<form method="post">

<div class="row">

<div class="col-sm-4"></div>

<div class="col-sm-4"><?php echo @$err;?></div>

</div>

<div class="row">

<div class="col-sm-4">Email ID</div>

<div class="col-sm-5">

<input type="email" name="e" class="form-control"/></div>

</div>

<div class="row">

<div class="col-sm-4">Password</div>

<div class="col-sm-5">

<input type="password" name="p" class="form-control"/></div>

</div>

<div class="row">

<div class="col-sm-4">Gender</div>

<div class="col-sm-5">

Male<input type="radio" name="gender" value="m" required/>

Female<input type="radio" name="gender" value="f"/>

</div>

</div>

<div class="row" style="margin-top:10px">

<div class="col-sm-2"></div>

<div class="col-sm-8">

<input type="submit" value="Login" name="save" class="btn btn-success"/>

</div>

</div>

</form>

**ADD\_NOTICE:**

<?php

extract($\_POST);

$conn = mysqli\_connect("localhost","root","","post\_mela");

if(isset($add))

{

if($details=="" || $sub=="" || $user=="")

{

$err="<font color='red'>fill all the fileds first</font>";

}

else

{

foreach($user as $v)

{

mysqli\_query($conn,"insert into notice values('','$v','$sub','$details',now())");

}

$err="<font color='green'>Notice added Successfully</font>";

}

}

?>

<h2>Add New Notice</h2>

<form method="post">

<div class="row">

<div class="col-sm-4"></div>

<div class="col-sm-4"><?php echo @$err;?></div>

</div>

<div class="row">

<div class="col-sm-4">Enter Subject</div>

<div class="col-sm-5">

<input type="text" name="sub" class="form-control"/></div>

</div>

<div class="row" style="margin-top:10px">

<div class="col-sm-2"></div>

<div class="col-sm-8">

</div>

<div class="row">

<div class="col-sm-4">Enter Details</div>

<div class="col-sm-5">

<textarea name="details" class="form-control"></textarea></div>

</div>

<div class="row" style="margin-top:10px">

<div class="col-sm-2"></div>

<div class="col-sm-8">

</div>

<div class="row">

<div class="col-sm-4">Select User</div>

<div class="col-sm-5">

<select name="user[]" multiple="multiple" class="form-control">

<?php

$sql=mysqli\_query($conn,"select name,email from male\_user");

while($r=mysqli\_fetch\_array($sql))

{

echo "<option value='".$r['email']."'>".$r['name']."</option>";

}

?>

</select>

</div>

</div>

<div class="row" style="margin-top:10px">

<div class="col-sm-2"></div>

<div class="col-sm-8">

</div>

<div class="row" style="margin-top:10px">

<div class="col-sm-2"></div>

<div class="col-sm-4">

<input type="submit" value="Add New Notice" name="add" class="btn btn-success"/>

<input type="reset" class="btn btn-success"/>

</div>

</div>

</form>

**UPDATE\_NOTICE:**

<?php

extract($\_POST);

if(isset($update))

{

mysqli\_query($conn,"update notice set subject='$sub',Description='$details' where notice\_id='".$\_GET['notice\_id']."'");

$err="<font color='blue'>Notice updated </font>";

}

//select old notice

$q=mysqli\_query($conn,"select \* from notice where notice\_id='".$\_GET['notice\_id']."'");

$res=mysqli\_fetch\_array($q);

?>

<h2>UPDATE NOTICE</h2>

<form method="post">

<div class="row">

<div class="col-sm-4"></div>

<div class="col-sm-4"><?php echo @$err;?></div>

</div>

<div class="row">

<div class="col-sm-4">Enter Subject</div>

<div class="col-sm-5">

<input type="text" name="sub" value="<?php echo $res['subject']; ?>" class="form-control"/></div>

</div>

<div class="row" style="margin-top:10px">

<div class="col-sm-2"></div>

<div class="col-sm-8">

</div>

<div class="row">

<div class="col-sm-4">Enter Details</div>

<div class="col-sm-5">

<textarea name="details" class="form-control"><?php echo $res['Description']; ?></textarea></div>

</div>

<div class="row" style="margin-top:10px">

<div class="col-sm-2"></div>

<div class="col-sm-8">

</div>

<div class="row">

<div class="col-sm-4">Select User</div>

<div class="col-sm-5">

<select name="user[]" multiple="multiple" class="form-control">

<?php

$sql=mysqli\_query($conn,"select name,email from male\_user");

while($r=mysqli\_fetch\_array($sql))

{

echo "<option value='".$r['email']."'>".$r['name']."</option>";

}

?>

</select>

</div>

</div>

<div class="row" style="margin-top:10px">

<div class="col-sm-2"></div>

<div class="col-sm-8">

</div>

<div class="row" style="margin-top:10px">

<div class="col-sm-2"></div>

<div class="col-sm-4">

<input type="submit" value="Update Notice" name="update" class="btn btn-success"/>

<input type="reset" class="btn btn-success"/>

</div>

</div>

</form>

**MANAGE\_USERS:**

<?php

$q=mysqli\_query($conn,"select \* from male\_user ");

$rr=mysqli\_num\_rows($q);

if(!$rr)

{

echo "<h2 style='color:red'>No any user exists !!!</h2>";

}

else

{

?>

<script>

function DeleteUser(id)

{

if(confirm("You want to delete this record ?"))

{

window.location.href="delete\_user.php?id="+id;

}

}

</script>

<h2 style="color:#00FFCC">All Users</h2>

<table class="table table-bordered">

<Tr class="success">

<th>Sr.No</th>

<th>User Name</th>

<th>Email</th>

<th>Mobile</th>

<th>Gender</th>

<th>Delete</th>

</Tr>

<?php

$i=1;

while($row=mysqli\_fetch\_assoc($q))

{

echo "<Tr>";

echo "<td>".$i."</td>";

echo "<td>".$row['name']."</td>";

echo "<td>".$row['email']."</td>";

echo "<td>".$row['mobile']."</td>";

echo "<td>".$row['gender']."</td>";

?>

<Td><a href="javascript:DeleteUser('<?php echo $row['id']; ?>')" style='color:Red'><span class='glyphicon glyphicon-trash'></span></a></td><?php

echo "</Tr>";

$i++;

}

?>

</table>

<?php }?>

**CHATTING**

<?php

session\_start();

include\_once "php/config.php";

if(!isset($\_SESSION['unique\_id'])){

header("location: login.php");

}

?>

<?php include\_once "header.php"; ?>

<html>

<body>

<div class="awrapper">

<nav class="navbar navbar-inverse navbar-fixed-top" style="background-color:#ffd700">

<section class="chat-area">

<header>

<?php

$user\_id = mysqli\_real\_escape\_string($conn, $\_GET['user\_id']);

$sql = mysqli\_query($conn, "SELECT \* FROM users WHERE unique\_id = {$user\_id}");

if(mysqli\_num\_rows($sql) > 0){

$row = mysqli\_fetch\_assoc($sql);

}else{

header("location: users.php");

}

?>

<a href="users.php" class="back-icon"><i class="fas fa-arrow-left"></i></a>

<img src="php/images/<?php echo $row['img']; ?>" alt="">

<div class="details">

<span><?php echo $row['fname']. " " . $row['lname'] ?></span>

<p><?php echo $row['status']; ?></p>

</div>

</header>

<div class="chat-box">

</div>

<form action="#" class="typing-area">

<input type="text" class="incoming\_id" name="incoming\_id" value="<?php echo $user\_id; ?>" hidden>

<input type="text" name="message" class="input-field" placeholder="Type a message here..." autocomplete="off">

<button><i class="fab fa-telegram-plane"></i></button>

</form>

</section>

</nav>

</div>

<script src="javascript/chat.js"></script>

</body>

</html>

**CHAT USER:**

<html>

<body>

<div class="wrapper">

<section class="users">

<header>

<div class="content">

<?php

$sql = mysqli\_query($conn, "SELECT \* FROM users WHERE unique\_id = {$\_SESSION['unique\_id']}");

if(mysqli\_num\_rows($sql) > 0){

$row = mysqli\_fetch\_assoc($sql);

}

?>

<a href="/down/index.php?option=login" class="back-icon"><i class="fas fa-arrow-left"></i></a>

<img src="php/images/<?php echo $row['img']; ?>" alt="">

<div class="details">

<span><?php echo $row['fname']. " " . $row['lname'] ?></span>

<p><?php echo $row['status']; ?></p>

</div>

</div>

<a href="php/logout.php?logout\_id=<?php echo $row['unique\_id']; ?>" class="logout">Logout</a>

</header>

<div class="search">

<span class="text">Select an user to start chat</span>

<input type="text" placeholder="Enter name to search...">

<button><i class="fas fa-search"></i></button>

</div>

<div class="users-list">

</div>

</section>

</div>

<script src="javascript/users.js"></script>

</body>

</html>

**BOOTSTRAP:**

/\*

\* Base structure

\*/

/\* Move down content because we have a fixed navbar that is 50px tall \*/

body {

padding-top: 50px;

}

/\*

\* Global add-ons

\*/

.sub-header {

padding-bottom: 10px;

border-bottom: 1px solid #eee;

}

/\*

\* Top navigation

\* Hide default border to remove 1px line.

\*/

.navbar-fixed-top {

border: 0;

}

/\*

\* Sidebar

\*/

/\* Hide for mobile, show later \*/

.sidebar {

display: none;

}

@media (min-width: 768px) {

.sidebar {

position: fixed;

top: 51px;

bottom: 0;

left: 0;

z-index: 1000;

display: block;

padding: 20px;

overflow-x: hidden;

overflow-y: auto; /\* Scrollable contents if viewport is shorter than content. \*/

background-color: #f5f5f5;

border-right: 1px solid #eee;

}

}

/\* Sidebar navigation \*/

.nav-sidebar {

margin-right: -21px; /\* 20px padding + 1px border \*/

margin-bottom: 20px;

margin-left: -20px;

}

.nav-sidebar > li > a {

padding-right: 20px;

padding-left: 20px;

}

.nav-sidebar > .active > a,

.nav-sidebar > .active > a:hover,

.nav-sidebar > .active > a:focus {

color: #fff;

background-color: #428bca;

}

/\*

\* Main content

\*/

.main {

padding: 20px;

}

@media (min-width: 768px) {

.main {

padding-right: 40px;

padding-left: 40px;

}

}

.main .page-header {

margin-top: 0;

}

/\*

\* Placeholder dashboard ideas

\*/

.placeholders {

margin-bottom: 30px;

text-align: center;

}

.placeholders h4 {

margin-bottom: 0;

}

.placeholder {

margin-bottom: 20px;

}

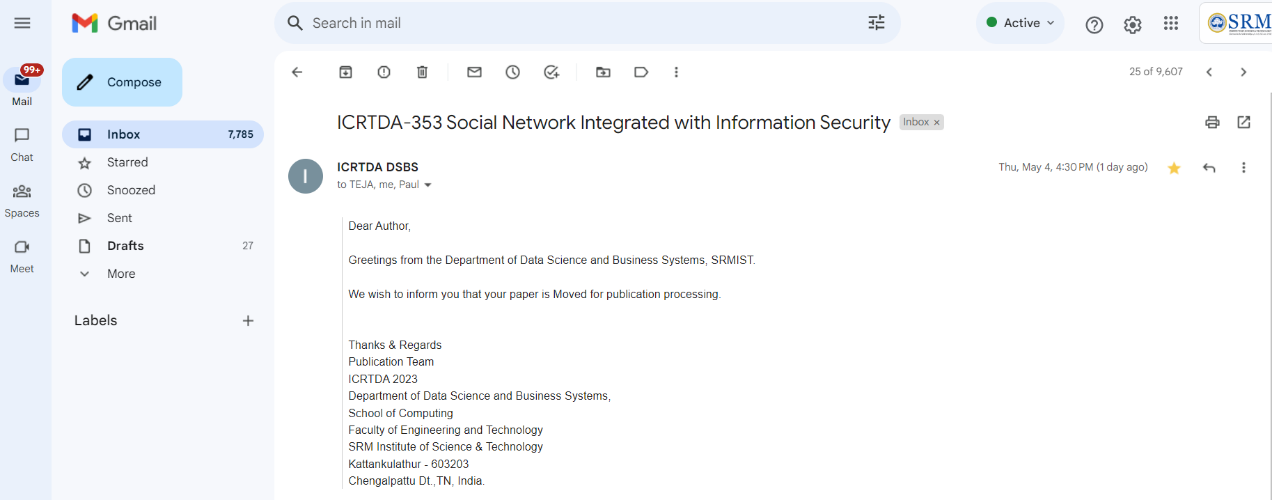
.placeholder img {

display: inline-block;

border-radius: 50%;

}

**PAPER PUBLICATION STATUS**



# **PLAGIARISM REPORT**

