

## Intelligent Security Platform for Multiple Access Controls

N. Chandra Sekhar Reddy<sup>1</sup>, K. Sai Prasad<sup>2</sup>, P. Srinivas Reddy<sup>3</sup>, K. Shekar<sup>4</sup>

<sup>1,2,3,4</sup>*Department of Computer Science and Engineering, MLR Institute of Technology, Hyderabad, India.*

### Abstract

*As everybody knows, our lives rotate around numbers like account numbers, pin numbers, pin codes, passwords and different bits of classified data that we have to recollect and monitor. Passwords for credit cards, ledgers, secret photographs, music and video, exceptionally profitable examined duplicates, drying's permit and visa numbers, and protection approach numbers are only inspecting of what we have to monitor. Because of our bustling life cycle, we cannot recall every one of them. Our end goal is to provide an exceptionally rich and intense answer for this issue this venture called "Intelligent Security Platform for Multiple Access Controls" has been planned and created. The reasoning is that we ought to have the capacity to recollect one secret word. The thought is to make that one secret word extremely secure, and through that watchword, we approach the more significant part of our different passwords. This application can safely store Bank Account Information. It utilizes a ground-breaking calculation and executes an exceedingly secure encryption instrument. ISPMAC turns into a fundamental through its universality, usability, security, and list of capabilities. It utilizes one of the least complicated and easy to understand interfaces and can store something other than passwords. It gives a lower cost answer to provide a high-security framework to store all the classified information.*

### 1. INTRODUCTION

Beginning with access control can be overpowering at first. Such vast numbers of specific terms and things to fold our head over. Understanding access control frameworks is indeed an achievable objective - particularly for controlling frameworks enables to manage, monitor and maintain who approaches a record on a web application.

The main role of the access controller is to guarantee fast, cooperative access control for approved users by limiting access for unapproved users. Basic Components of Access Control Systems are broadly in sort and complicated quality. Most access control frameworks comprise of in any event the accompanying vital parts: client-side and administrator side. User-side components deal with information storage and accessing data records with some security by a user interface. Administrator-side elements include assessment management dashboard, integration, and API. Administration dashboard or appearance where officials can supervise, maintain and regulate access for representatives, guests or staff. Combinations and API can be utilized to automate manual work processes and make activities less inclined to mistakes.

It is a reality all around recognized, that secret word-construct confirmation concerning the web is unstable. One primary, if not the essential, concern with secret word authentication is the significant weight of picking secure, random passwords over every one of the destinations that depend on password verification. An extensive collection of proof proposes clients have conceivably, judiciously surrendered, choosing straightforward passwords and reusing them crosswise over targets.

An intelligent security platform for multiple access controllers [ISPMAC] is an outstanding approach to monitoring every one of a kind of access controllers, or on the other hand, a passphrase that you have made for your different online records without writing down on a bit of paper and taking a chance with that others will see them. ISPMAC, an online platform that provides security for passwords and data records such as image files, audio files, and video files, and so forth.

## 2. LITERATURE REVIEW

In the last decade, various graphical secret vital plans have been proposed, prompted by the agreement of enhanced access controller <sup>ea2se</sup> 1 of use, while in the meantime improving quality against speculating assaults. Like substance passwords, graphical passwords are data-based confirmation devices where customers enter a customary text word as the secret password of their existed accounts. The passwords include alphanumeric and additionally extraordinary console characters for protecting a lot of online accounts which clients have to remember with human memory.

The essential requirement for an entrance controller is that anchoring passwords are relied upon to be simpler to review, more averse to be composed down and can possibly give a more energizing space than a content based secret key. Specialists are ceaselessly presenting new thoughts, ideas, and highlights in the field of graphical confirmation. There are as of now numerous methodologies have been proposed in display times. Blonder [1] gave the underlying motivation behind the graphical secret word in 1996. In his strategy, a UI is possible with one foreordained picture and required to choose at least one existing positions on showed picture in a specific request to get to the limited assets. The basic disadvantage of this framework is that clients can't click subjectively on the foundation. The remarkable secret word space was not considered by the creator either. Wiedenbeck et al. [2] proposed Pass Point technique in which widened Blonder's idea by abstaining from as far as possible and empowering self-confident pictures to be used. Accordingly, a customer can tap on wherever on a photo (instead of some pre-portrayed areas) to influence one mystery word for getting to tied down data, with the common mystery being related to or made out of pictures, parts of pictures, or diagrams. [3]

### 2.1 Existing System

In the current system quite often, people write down confidential account numbers and passwords on paper and carry it along with them to remember those personal details, passwords. We also use a general-purpose email facility as a data store for storing all of their sensitive data so that they can access them through the internet from any place. Usability issues often significantly impact the real-world security of the system.

Despite a large number of options for authentication, text passwords remain the most common choice for several reasons. For example, they are comfortable and inexpensive to implement; are familiar to virtually all users enable clients to validate themselves while maintaining a strategic distance from security issues that have been raised about biometrics; and have the upside of conveyability without, for instance, carrying physical tokens. Be that as it may, content passwords likewise experience the ill effects of both security and ease of use hindrances — for example, passwords are regularly hard to recall, and are unsurprising if client decision is permitted. [3]

At the point when content watchword clients embrace dangerous adapting techniques, for example, reusing passwords crosswise over records to help with memorability, the subsequent decline in security cannot be expertly tended to by only fortifying, in detachment, the hidden specific security parts of a framework. User interface design decisions may unintentionally sway user behavior, usually towards less secure behavior. Successful authentication solutions must thus also include improved usability design based on appropriate research considering the abilities and limitations of the target users.

#### Disadvantages:

- A manual approach, for example, recording classified record numbers and passwords on paper to recall them is counterproductive to keeping up privacy and security.
- For a normal individual, it is important to remember much data.
- Unauthorized persons can gain access to confidential data.
- General purpose email systems are highly vulnerable to security threats and often become targets for hacking.

### 2.2 Proposed Work

The proposed structure ISPMAC is an extraordinary web application which can securely store private data like passwords for Documents, financial balances, top-secret photographs, music, and video, hugely significant examined duplicates, driver's permit and travel permit numbers, and protection approach numbers are only testing of what we have to monitor. As each snippet of data saved into the ISPMAC framework, a different database passage is complete. At the season of entering private information and data relying upon the kind of data it is, the structure will provoke the end client for related data. Afterward, when the end client needs to recover information, the client should get to the application utilizing a single secret word. Application's recovery interface will show every passage by name, yet classify and bunch together kinds of sections, for example, financial balances, charge card accounts, and different passwords.

#### **Advantages:**

- ISPMAC enables its end clients to make one focal database containing a wide range of sorts of sections (ledgers, charge cards, secret word sites, etc.)
- This exceptionally secure and safe application enables its end clients to classify their private information sections and afterward amass them, so the entirety of their ledgers, site passwords, or checked duplicates are effortlessly retrievable and stay efficient.
- For an average person, there will be no need to memorize much information. Hence there will be no need to write down confidential record numbers and passwords on paper to recall them which is counterproductive to keeping up privacy and security.
- The philosophy of having “one password which is very secure and through that single password have access to all of the other passwords and confidential information” can be quickly realized.

#### **Features of the Framework:**

- This platform is protected based on a standard login procedure. It is essential to secure the passwords that allow access to other confidential information.
- The intention behind building this tool is to simplify the job of the regular user by remembering just one password.
- It provides an efficient solution to store confidential data.
- This highly secure and safe application allows its end users to categorize their personal sensitive data entries.

### **3. Implementation**

#### **3.1 Problem Definition**

##### **Error management in Extreme conditions:**

The proposed framework should deal with special cases that begin at low-level parts and constraints at abnormal state segments. The abnormal state parts in the proposed framework should deal with special cases that happen while interfacing with the database server, IO Exceptions. The end client won't have any constraints at low-level. At the point when low-level Exceptions emerges, the client ought to be appeared with a fitting message. Blunders that happen amid information passage ought to be taken care of by performing customer side approvals. In the proposed framework all customer side approvals will be finished utilizing JavaScript.

##### **Quality Issues:**

Quality issues allude to how dependable and strong should the framework be? While building up the proposed technique, the designer must have the capacity to ensure their obligation for exchanges with the goal that exchanges can be done precisely. The capacity of the framework to distinguish disappointments and recuperation from those disappointments alludes to the accessibility of the framework. Strength alludes to the measurements of a framework giving data when simultaneous clients are asking for data. As the proposed framework's ability of taking care of the different special case, it is solid, and it will be created utilizing JSP which bolsters multi-threading. Subsequently it fulfills the solicitations from simultaneous clients. In this way, it is powerful.

##### **Framework alteration:**

The proposed framework is not actualizing on the web correspondence amongst client and head so it tends to be expanded and this refreshing should be possible by any designer comfortable with determined equipment and programming requirements took after for improvement of the proposed framework. Security and secrecy are the best most worries of the customer. The proposed framework ought to give the accompanying. The director ought to be provided with id and secret word for secure access of data in regards to client's administration. Every User ought to likewise be given code and secret word for controlled access of data with respect to their anchored data like individual data, sound and video lockers.

### **3.2 Modules Description**

The framework of ISPMAC contains six modules which are

- User Management module
- Security System module
- Personal Information Locker module
- Bank Account Information Locker Module
- Image, Video and Music Locker Module

#### **User Management Module: -**

The administrator can access this module to make user management simple. The administrator has to approve or reject the registered users after communicating with the users. Even after approval, he can lock and unlock the users. The administrator has control to verify the list of locked and unlocked users.

#### **Security System Module:**

This module adds security features to the information stored by the user like their username, password, and personal banking information. Data encryption protects user data from getting into wrong hands. Decryption mechanism is applied to evert the encrypted data to a human-readable format.

#### **Personal Information Locker Module:**

Users can store their personal information like email ID, password, pancard, passport, visa and driving permit subtle elements and whenever he can see and erase those points of interest in the event that he needs. This module is dependent on Security system module to encrypt and decrypt the email id & password, pan card, passport & driving license details.

#### **Bank Account Information Locker Module:**

Users can access this module to store personal banking information is like bank account details, net banking details & insurance policies details and he can view those details if he needed. This module includes security system operations to encrypt & decrypt the details like a bank account, net banking details & insurance policy details.

#### **Image, Video and Music Locker Module:**

The users can access this module to store the Images like a scanned or original copy of images, he can upload audio files which required security, and he can also upload video files which needed protection. If the user required those stored images, audio files & video files could be download.

### **3.3 System Architecture**

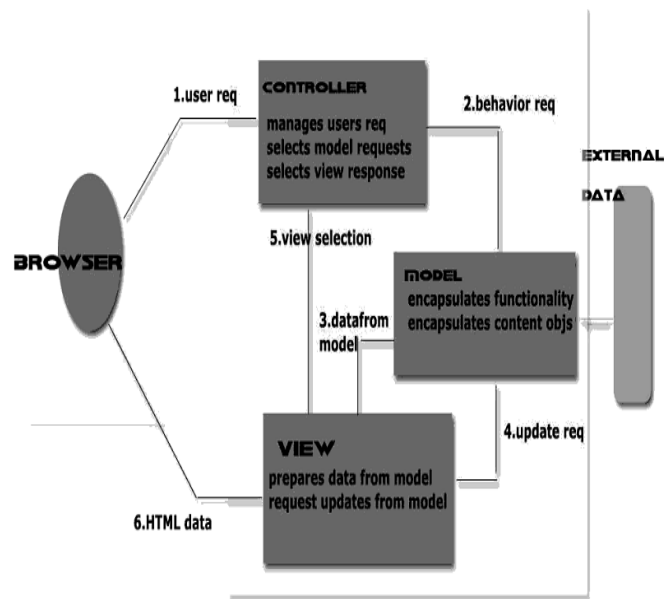


Figure : 1 System Architecture of ISPMAC

Layerd Architecture

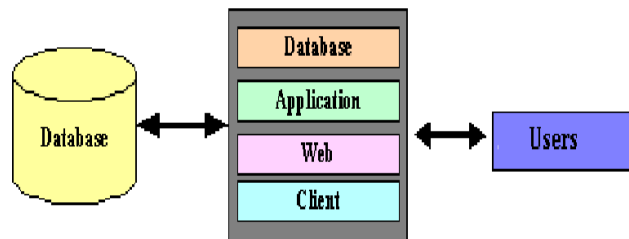


Figure 2: Layers of ISPMAC Architecture.

**Database Layer:** Contains the information and database-related articles like put away methods, triggers, bundles.

**Application Layer:** Contains the items tending to the business basis; Most of the mediocre Java objects will be here inside the application layer.

**Web Interface Layer:** It will take a shot at the online server; It contains the website pages (JSPs) of the application which can associate with the front-end programs

**Client Layer:** Contains the internet browser that expresses and communicates with the web-server

**3. RESULTS**

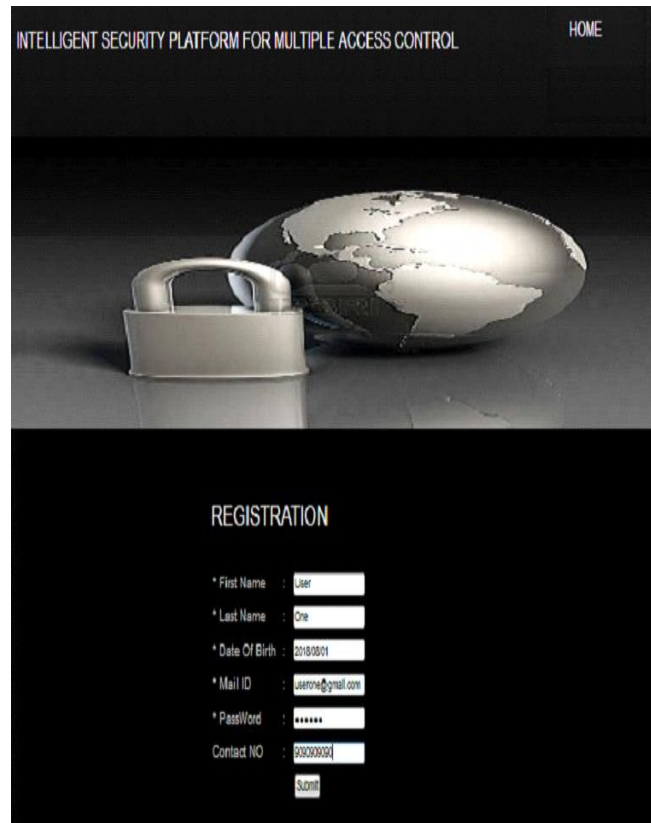


Figure: 3 Registration page of ISPMAC

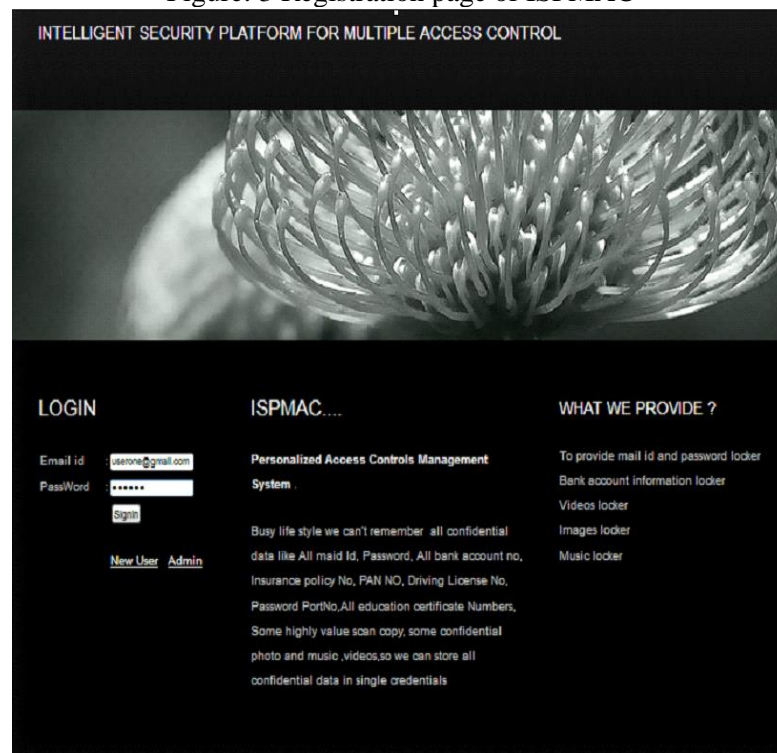


Figure: 4 User Login page of ISPMAC

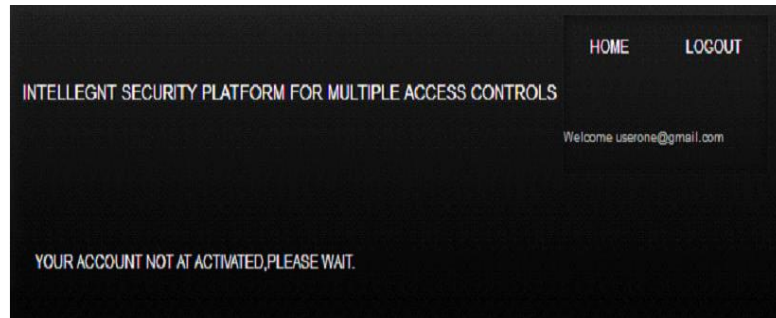


Figure: 5 User Front page of ISPMAC before activation

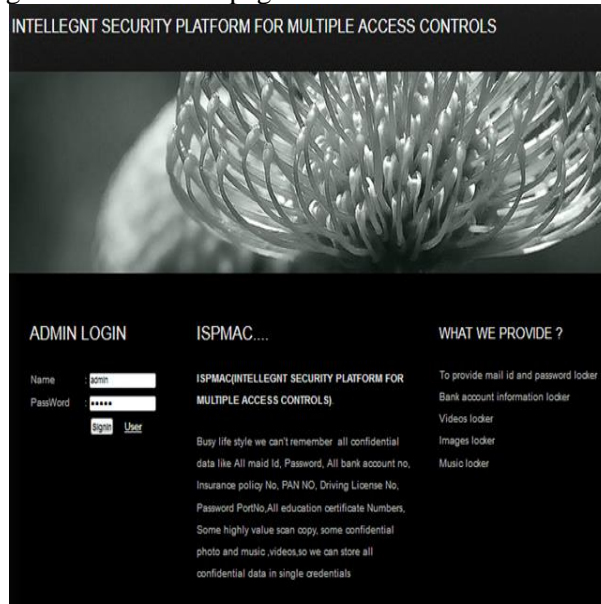


Figure: 6 Admin Login page

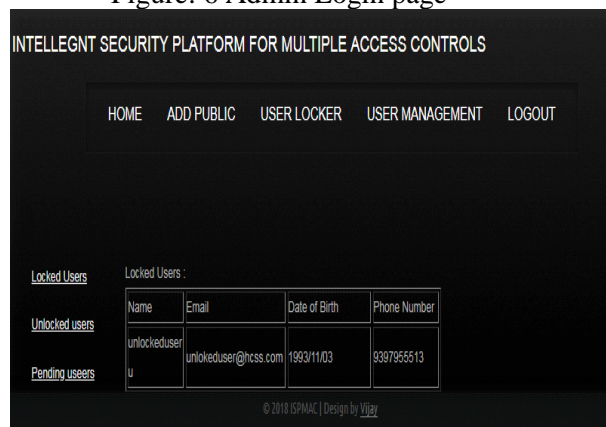


Figure: 7 Locked users page of the admin

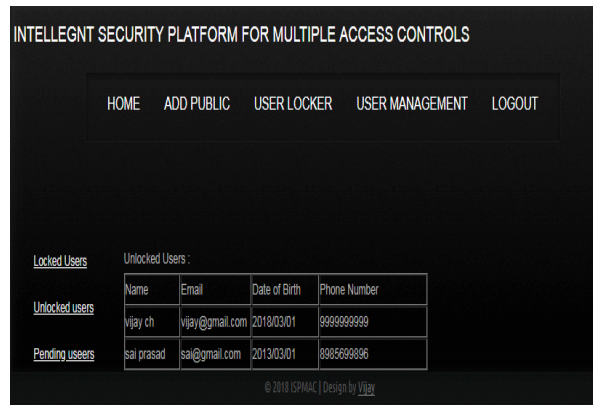


Figure: 8 Unlocked users page of Admin

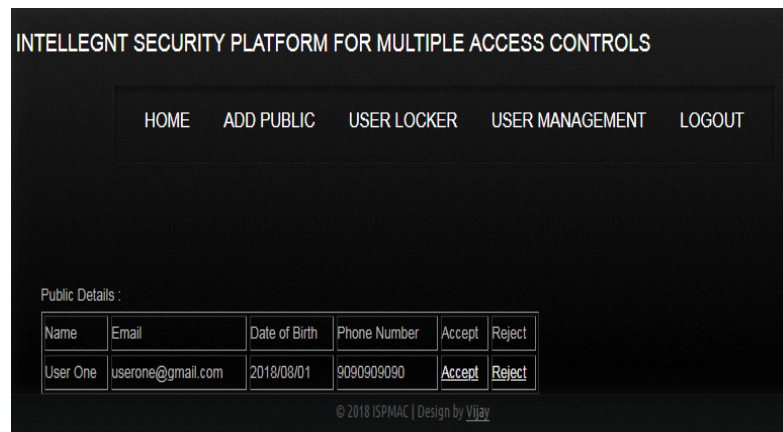


Figure: 9 Available Users page when a new user registered.

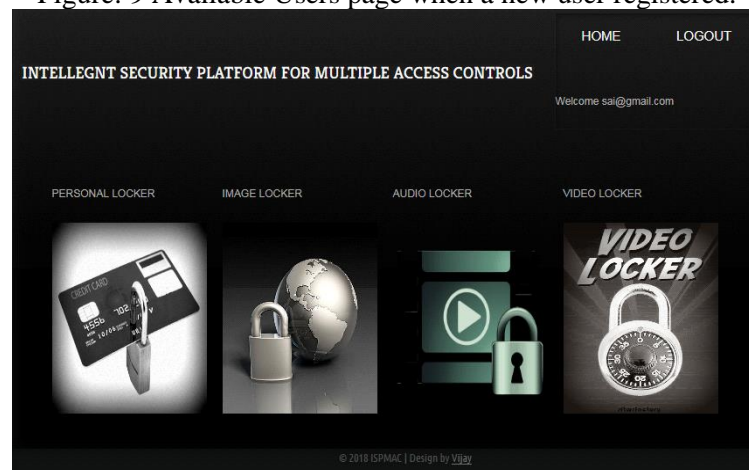


Figure: 10 Homepage of Users after admin approval.



**BANK ACCOUNT**      **NEW ACCOUNT**      **EXISTED ACCOUNT DETAILS**

INSURANCE POLICY

MAIL ID'S

PAN CARD

PASSPORT

DRIVING LICENCE

\* Ac Holder Name :

\* Bank Name :

\* Branch Name :

\* Acc Number :

**Atm Card Details**

Atm Card Number(16 Digit's) :

Atm Cvv(3 Digit's) :

Atm Pin :

**Netbanking Details**

Name :

Pswd :

Pin :


© 2018 ISPMAC | Design by Vijay

Figure: 11 webpage to store Bank account details of users.

HOME      LOGOUT

INTELLIGENT SECURITY PLATFORM FOR MULTIPLE ACCESS CONTROL

Welcome sai@gmail.com



**BANK ACCOUNT**      **SBI ACCOUNT DETAILS**      **EXISTED ACCOUNT DETAILS**

INSURANCE POLICY

MAIL ID'S

PAN CARD

PASSPORT

DRIVING LICENCE

\* Ac Holder Name : sai      [sbi](#) For sai

\* Bank Name : sbi

\* Branch Name : dundigal

\* Acc Number : 9838527410

**Atm Card Details**

Atm Card Number : 7418520820963

Atm Cvv : 321

Atm Pin : 2589

**Netbanking Details**

Name : sai

Pswd : 9832

Pin : 9868

Figure: 12 Existed bank account details of Users.

Figure: 13 Insurance Policy form for Users.

Figure: 14 Existed Insurance Policy details of the user.

Figure: 15 Existed Mail id's details of the user.

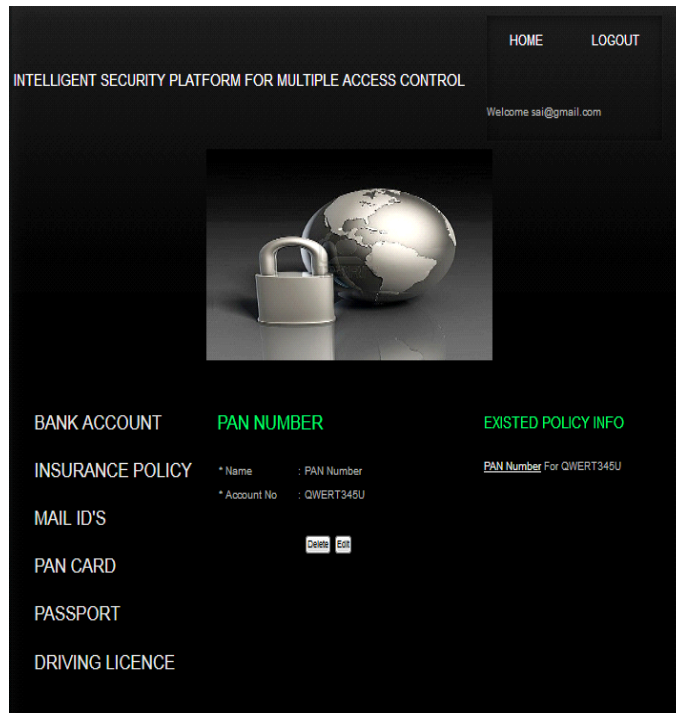


Figure: 16 Existed PAN card details of the user.

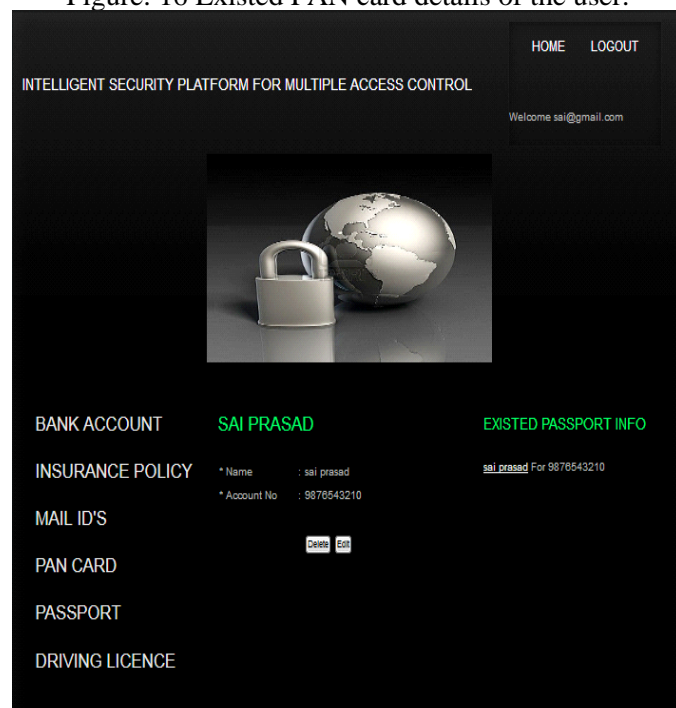


Figure: 17 Existed Passport details of the user.

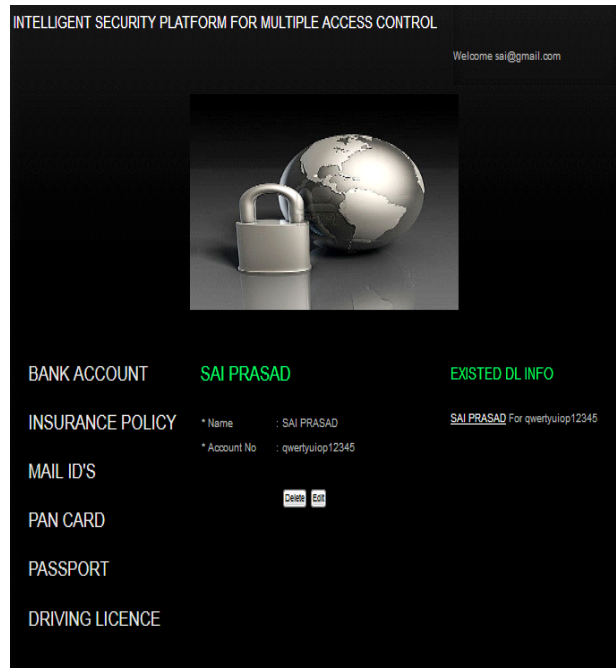


Figure: 18 Existed Driving License details of the user.

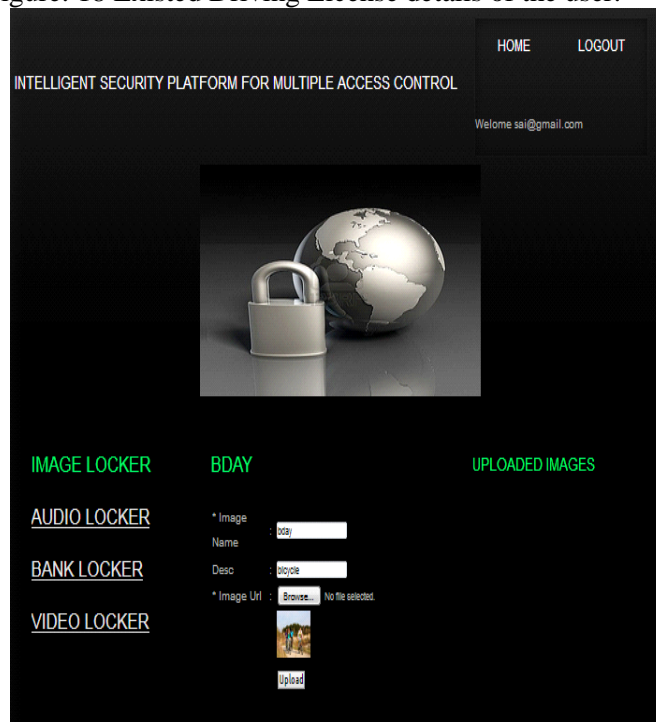


Figure: 19 webpage for uploading an image.

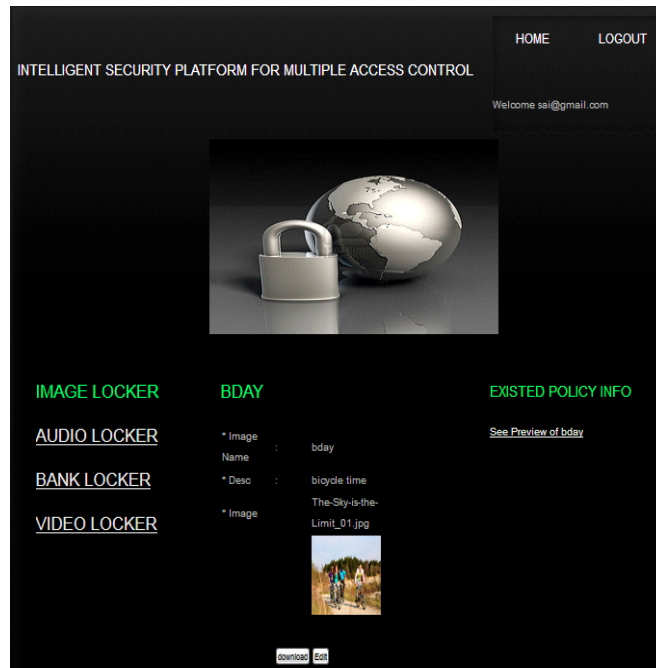


Figure: 20 webpage for retrieving an image.

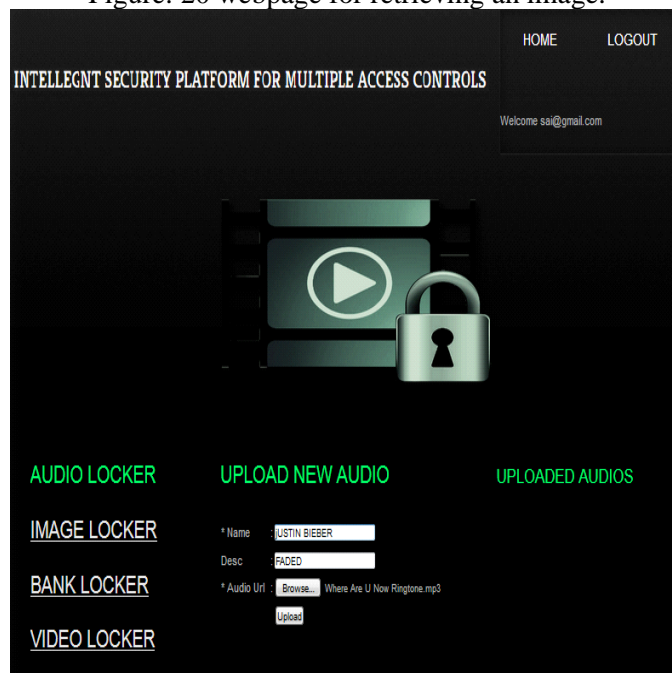


Figure: 21 webpage for uploading an audio file.

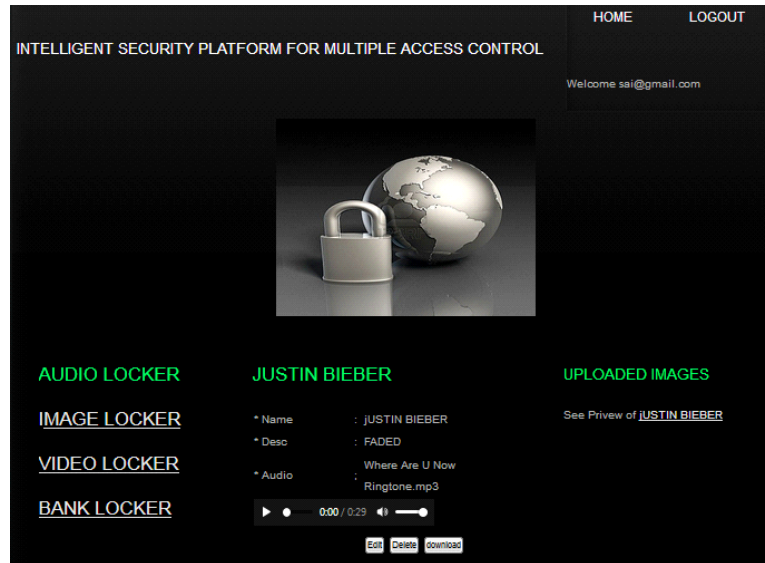


Figure: 22 webpage for online playing an audio file.

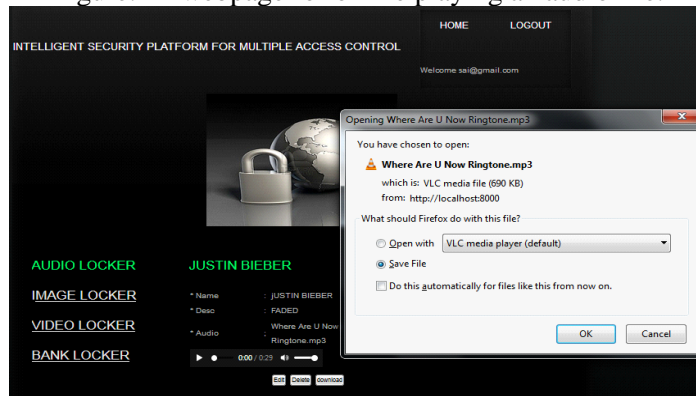


Figure: 23 webpage for downloading the audio file from ISPMAC.

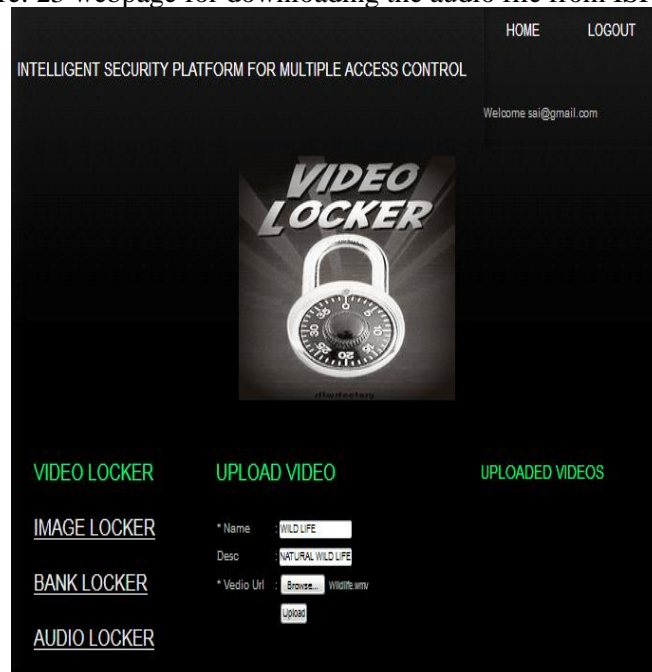


Figure: 24 webpage for uploading a video file.

#### 4. CONCLUSION AND FUTURE ENHANCEMENT

##### Conclusion

The “Intelligent Security Platform for Multiple Access Controls” is web-based application software that has been computed successfully and was also tested successfully by taking “test cases.” This platform is protected based on a standard login procedure. It is essential to secure the passwords that allow access to other confidential information. ISPMAC enables its end clients to make one focal database containing a wide range of sorts of sections (ledgers, charge cards, secret word sites, etc.)

The goals that are achieved by the software are:

- Instant Access to multiple access control platform.
- Less processing time for retrieving the required information.
- A recognizable method to diminish misuse of private information.
- It is ease of use to perform desired operations.

##### Confinements

- ISPMAC is limited to protect all the personal information, images, audios, and videos by using single secure locker.
- Registrations of clients should be processed by the Admin first then they can log in into the application.
- Lack of two-way authentication.

##### Future Enhancement

- We can implement a tool which will able to store all the personal information, images, audios, and videos. For each info, there may be a separate locker.
- We can implement two-way authentication for our ISPMAC.
- We can extend this project by providing multiple lockers, each locker password is stored in the form encrypted format.
- The further work is to figure out how to make full utilization of Globus' resources improvement capacity to upgrade the web administration's performance and proficiency.

#### REFERENCES

1. G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent-5559961, Ed. The United States, 1996.
2. Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon, “Passpoints: design and longitudinal evaluation of a graphical password system,” *International Journal of Human-Computer Studies*, 63:102–127, July 2005.
3. “Graphical Passwords: Learning from the First Generation,” Robert Biddle, Sonia Chiasson, P.C. van Oorschot, Version: October 2, 2009. Technical Report TR-09-09, School of Computer Science, Carleton University, Ottawa, Canada.
4. Chandrasekar S, Dakshinamurthy R, Seshakumar P G, Prabavathy B, ChitraBabu, “A Novel Indexing Scheme for Efficient Handling of Small Files in Hadoop Distributed File System”, in *International Conference on Computer Communication and Informatics (ICCCI -2013)*, Jan. 04 - 06, 2013, Coimbatore, INDIA,2013.
5. Kashi Sai Prasad, S Pasupathy, "Real-time Data Streaming using Apache Spark on Fully Configured Hadoop Cluster", *J.Mech.Cont.& Math. Sci.*, Vol.-13, No.-5, November-December (2018) Pages 164-176.
6. Sirisha, N., Kiran, K.V.D., "Stock exchange analysis using Hadoop user experience (Hue)", (2018) *Proceedings of the International Conference on Intelligent Sustainable Systems, ICISS 2017*, pp. 1141-1144.
7. Prasad, K.S., Reddy, N.C.S. & Puneeth, B.N. A Framework for Diagnosing Kidney Disease in Diabetes Patients Using Classification Algorithms. *SN COMPUT. SCI.* 1, 101 (2020).

8. G. Prabhakar Reddy, K. Sai Prasad, N. Chandra Shekar Reddy and R. Karthik, 2018. Privacy Preserving and Data Publishing using Tuple Grouping Algorithm. Journal of Engineering and Applied Sciences, 13: 930-933.