ISSN (Online): 2455-7013
Asian Journal of Management, Engineering & Computer Sciences (AJMECS)
Vol. 1(1), January 2016: 1-12
Journal's URL: http://www.crsdindia.com/ajmecs.html
Email: crsdindia@gmail.com

ORIGINAL ARTICLE

Graphical User Authentication by Secured Intrusion Prevention Implementation in Storage

Asifahmed Algur
Dept. of Computer Science,
P.A. College of Engineering, Mangalore, Karnataka, India.
Email: asifalgur005@gmail.com

ABSTRACT

Secure intrusion prevention in a storage using graphical user authentication is an application where a user can make use of the storage system to store any type of files in an common storage and only authenticated users are permitted to view their own files and if someone tries to view others file then he will be treated as intruder and he/she will be blocked and left with a message contact to admin. Graphical user authentication adds an extra level of security which uses an image for user authentication. Plenty of threats & security attacks are being launched against web applications everyday, which are aimed to gain unauthorized access to the sensitive information from the back-end database. So we develop a system where only authorized client can access their data from the database using intrusion prevention technique and graphical user authentication technique.

Key words: *Secure intrusion, Graphics, User Authentication*

Received: 22nd Nov. 2015, Revised: 4th Dec. 2015, Accepted: 9th Dec. 2015

How to cite this article:
Algur A. (2016): Graphical User Authentication by Secured Intrusion Prevention Implementation in Storage. AJMECS, Vol. 1[1]: January, 2016: 1-12.

INTRODUCTION

Intrusion prevention system in our project disallows the unauthenticated client from accessing the data stored in the database or storage and the unauthenticated client/user will be blocked if he/she tries to access the data stored in the database. There will be a common database for the clients/users where they can store the data and only they can access the data. Intrusion prevention system is used for the security purposes, these systems they never allow the unauthenticated client/user to access the data stored in the database. An increasing number of organizations use information systems to conduct their core business activities. As a result, the frequency and magnitude of intrusion incidents have increased significantly. Intrusion attacks have many causes, such as malware (e.g., worms, spyware), unauthorized access to systems and misuse of privileges or attempt to gain additional privileges. While some incidents are malicious in nature, others are not. To reduce the exposure to both types of intrusion threats, organizations need intrusion detection systems (IDS) and intrusion prevention systems (IPS). Although 72 percent of companies already use IDS and IPS, the number of entities experiencing intrusion incidents has grown from 58 percent in 2000 to 65 percent in 2005.This indicates that it is important to know the different types of security technologies that are available and the effectiveness of each type in reducing the risk of intrusion threats to implement a security system that best suits the needs of the organization.

A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA).The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, we have developed authentication methods that use pictures as passwords. But we are using this graphical user authentication or graphical password authentication technique to add the extra level of security so that authenticated client can access the data stored in the database.Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text; psychological studies supports such assumption. Pictures are generally easier to be remembered or recognized than text. In addition, if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text-based schemes and thus presumably offer better resistance to dictionary attacks. Because of these advantages, there is a growing interest in graphical password. In addition to workstation and web log-in applications, graphical passwords have also been applied to ATM machines and mobile devices. Graphical user authentication technique in our project is to select an image at the time of registration and at the time of client login the authenticated client needs to select the same image for authentication.

Our project focuses on how unauthenticated clients can be prevented from intruding into the storage and to allow only authenticated client to have access to their own data in the database or storage otherwise they will be blocked and later they need to contact the administrator if they want to activate your ID.

LITERATURE SURVEY

Our project mainly uses two techniques intrusion prevention and graphical user authentication; I had done a survey on these techniques.

As the network technology is increasing rapidly, the security of that technology is becoming a need for survival for an organization. Most of the organizations are depending on the internet to communicate with the people and systems to provide them news, online shopping, email, credit card details and personal information. Due to the rapid growth in the technology and widespread use of the Internet, a lot of problems have been faced to secure the system's critical information within or across the networks because there are millions of people attempting to attack on systems to extract critical information. A huge number of attacks have been observed in the last few years. Intrusion Detection and Prevention Systems (IDPS) play an immense role against those attacks by protecting the system's critical information. As firewalls and anti viruses are not enough to provide full protection to the system, organizations have to implement the IDPS to protect their critical information against various types of attacks.

Intrusion means to interrupt someone without permission. Intrusion is an attempted act of using computer system resources without privileges, causing incidental damage. Intrusion Detection means any mechanism which detects the intrusive behavior. Intrusion Detection System (IDS) monitors network traffic and its suspicious behavior against security. If it detects any threat then alerts the system or network administrator. The objective of IDS is to detect and inform about intrusions. An ID is a set of techniques and methods that are used to detect suspicious activities both at the network and host level. There are two main types of Intrusion Detection System, Host Based Intrusion Detection Systems (HIDS) and Network Based Intrusion Detection Systems (NIDS).

IPS is an advance combination of IDS, personal firewalls and anti-viruses etc. The purpose of an Intrusion Prevention System (IPS) is not only to detect an attack that is trying to

interrupt, but also to stop it by responding automatically such as logging off the user, shutting down the system, stopping the process and disabling the connection etc. Similar to IDS, IPS can be divided into two types, i.e. Host-Based Intrusion Prevention Systems and Network-Based Intrusion Prevention Systems [1].If we merge both IDS and IPS on a single host then it is known as a Host-based Intrusion Detection and Prevention System (HIDPS). Host-based Intrusion Detection and Prevention System (HIDPS) relates to processing data that originates on computers themselves, such as event and kernel logs. HIDPS can also monitor that which program accesses which resources and might be flagged. HIDPS also monitors the state of the system and makes sure that everything makes sense, which is basically a concept of anomaly filters. HIDPS normally maintains a database of system objects and also stores the system's normal and abnormal behavior. The database contains important information about system files, behavior and objects such as attributes, modification time, size, etc. If any suspicious or anomaly behavior occurs then it generates an alarm and takes some appropriate response against detected threat or attack.

Intrusion detection is network-based when the system is used to analyze network packets. Network based Intrusion Detection and Prevention System (NIDPS) capture the network traffic from the wire as it travels to a host. This can be analyzed for a particular signature or for unusual or abnormal behaviors. Several sensors are used to sniff the packets on network which are basically computer systems designed to monitor the network traffic. If any suspicious or anomaly behavior occurs then they trigger an alarm and pass the message to the central computer system or administrator (which monitors the IDPS) then an automatic response is generated. There are further two types of NIDPS. Promiscuous-mode network intrusion detection is the standard technique that "sniffs" all the packets on a network segment to analyze the behavior. In Promiscuous-mode Intrusion detection systems, only one sensor is placed on each segment in the network. Network-node intrusion detection system sniffs the packets that are bound for a particular destination computer. Network-node systems are designed to work in a distributed environment [2].

Harley [2] defines the difference between host based and network based intrusion detection and prevention system. This paper describes two types of network intrusion detection system: Promiscuous-mode and Network-node. The main disadvantage observed is that this IDS only responds to the signature based detected attacks but not to the anomaly based detected attacks. So still there is a need of human interaction who took real time action to resolve issue [2]. Authentication is process of determining whether someone or something is, in fact who or what to be declared. For authentication mostly textual passwords are used. Passwords are the most commonly used method for identifying users in computer and communication systems. Typically, passwords are strings of letters and digits, i.e., they are alpha-numeric. Such passwords have the disadvantage of being hard to remember. Graphical passwords, which consist of some actions that the user performs on an image. Such passwords are easier to remember, but are vulnerable to shoulder surfing (which consists of simply watching a user login).

Passwords are mostly widely used form of authentication. Commonly used methods for authentication are as follows:

1. Authenticate Using Username and Password.
2. Authenticate Using a Certificate deployed to the mobile device.
3. Authenticate using one-time password or security tokens.
4. Authenticate using Smart Card.

Authentication is more essential for the security purpose. Upto this password can be easily guessed by any third person. Authentication is direct need of each and every person's / organization; it is essential for a person's/organization not because it copes with security threats, the reason it deals with develops policies, procedure and

mechanisms that provide administrative, physical and logical security. Different organizations have different authentication requirements and so they set different authentication according to their requirement type. The main goal of authentication to secure their data/system from third (unknown) person. Authentication being used increasingly in military and government agencies, hospital and other business settings [3].

Two new authentication schemes authenticate the user by session passwords which are used only once. Once the session is terminated, the session password is no longer useful. For every login process, users input different passwords. The session passwords provide better security against dictionary and brute force attacks as password changes for every session. But in this same problem is occur that every time user has to enter password again and again. It is too hard to remember password and as it is the session password it is for the particular time only [4].

To remove the drawback of textual password removed by graphical password schemes which provide a way of making more user friendly passwords, while increasing the level of security, they are vulnerable to shoulder surfing .Here text was combine with image and color to generate the session password and every time user wants to enter new password as session ends. Two authentication techniques (pair-based authentication scheme and hybrid textual authentication scheme) for engendering the session passwords. Same problem is here too as previously comes. Drawbacks associated with the textual passwords such as brute-force and dictionary attacks and same this problem held with graphical passwords which includes shoulder-surfing and are very expensive to implement. Two authentication techniques (pair-based authentication scheme and hybrid textual authentication scheme) for engendering the session passwords [5].

Alpha numeric password were first introduced in the 1960s for security purpose that secure the confidential data .In alpha numeric password the password are :

1. The password should be at least 8 characters long.
2. The password should not be easy to relate to the user.
3. The password should not be a word that can be found in dictionary or public dictionary.
4. Ideally, the user should combine upper and lower case letters and digits.

Alpha-numeric password is the dictionary attack. Passwords are used by user are mostly common words or phone no., name etc. These types of passwords are easily guessed or crack by third person.

Because human beings live and interact in an environment where the sense of sight is predominant for most activities, our brains are capable of processing and storing large amounts of graphical information with ease. While we may find it very hard to remember a string of fifty characters, we are able easily to remember faces of people, places we visited, and things we have seen. These graphical data represent millions of bytes of information and thus provide large password spaces. Thus, graphical password schemes provide a way of making more human-friendly passwords while increasing the level of security [6][7].

User authentication is a fundamental component in most computer security contexts. It provides the basis for access control and user accountability [8]. While there are various types of user authentication systems, alphanumerical username/passwords are the most common type of user authentication. They are versatile and easy to implement and use.Alphanumerical passwords are required to satisfy two contradictory requirements. They have to be easily remembered by a user, while they have to be hard to guess by impostor [9]. Users are known to choose easily guessable and/or short text passwords, which are an easy target of dictionary and brute-forced attacks [10,11,12]. Enforcing a strong password policy sometimes leads to an opposite effect, as a user may resort to

write his or her difficult-to-remember passwords on sticky notes exposing them to direct theft.

In the literature, several techniques have been proposed to reduce the limitations of alphanumerical password. One proposed solution is to use an easy to remember long phrases (passphrase) rather than a single word [13]. Another proposed solution is to use graphical passwords, in which graphics (images) are used instead of alphanumerical passwords [14]. This can be achieved by asking the user to select regions from an image rather than typing characters as in alphanumeric password approaches.

Graphical passwords refer to using pictures (also drawings) as passwords. In theory, graphical passwords are easier to remember, since humans remember pictures better than words [15]. Also, they should be more resistant to bruteforce attacks, since the search space is practically infinite.

In general, graphical passwords techniques are classified into two main categories: recognition-based and recall based graphical techniques [14]. In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage. In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

Passfaces is a recognition-based technique, where a user is authenticated by challenging him/her into recognizing human faces [16]. An early recall-based graphical password approach was introduced by Greg Blonder in 1996 [17]. In this approach, a user creates a password by clicking on several locations on an image. During authentication, the user must click on those locations. Pass Points builds on Blonders idea, and overcomes some of the limitations of his scheme [9]. Several other approaches have been surveyed in the following paper [14]. The above surveyed papers gave me the idea about the intrusion prevention system and graphical user authentication and I developed a project where I make use of traditional user registration system for the users and added an additional level of security called the graphical user authentication that require the user to select an image from the system at the time of registration and during the client login the user needs to select the same image that was selected during the time of registration so as to prevent from intrusion in the storage.

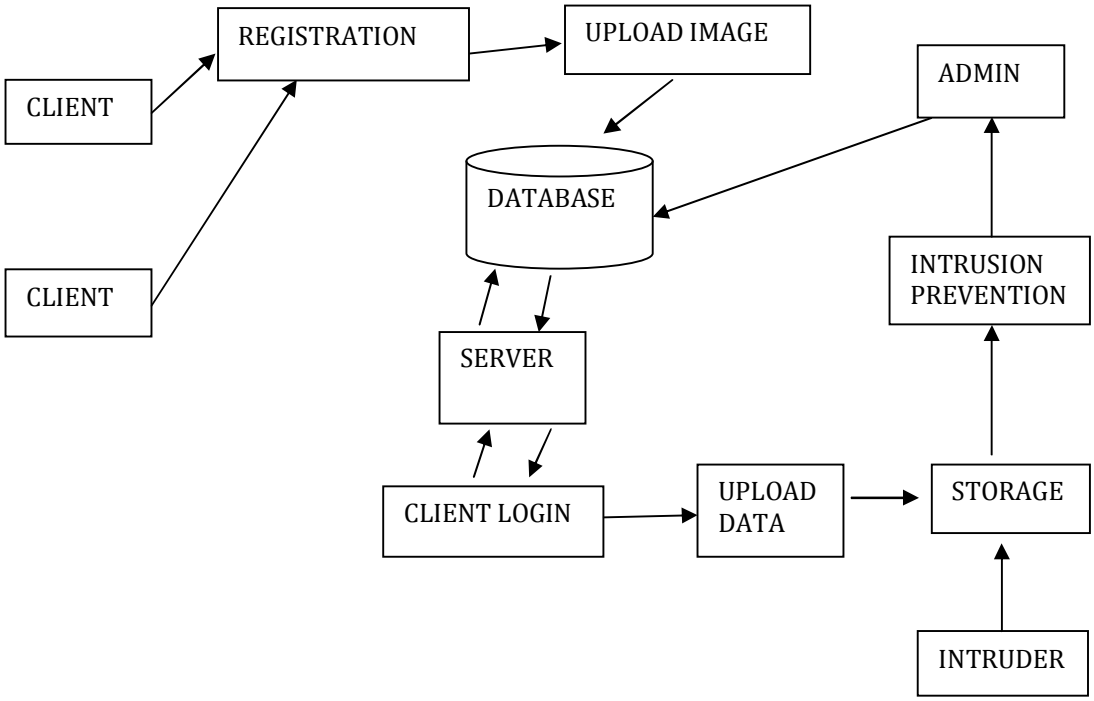
IMPLEMENTATION

As we know the conventional system of registering the user is becoming attack prone in which a user registers himself/ herself with a username, password etc.at the time of login the user enters the correct username and password that was provided by the user at the time of registration. In this case if a registered users credentials (username and password) is known to any other client, he/she may misuse with that credentials and may easily intrude into storage and access files. With this existing system in mind I designed a system in which only authenticated client can access their own data from the storage using image authentication technique where I made use of conventional registration system along with the user will upload an image into the database at the time of registration and at the time of login the client will enter his/her credentials along with that the user will upload the same image that was uploaded at the time of registration thus the proposed system avoids the intruder from accessing the data.

The description of the architecture diagram includes the client in order to store data in the storage the client must first register in the system by filling the appropriate fields and by uploading image of his/her choice and the credentials and the image will be stored in the database then later the client can login into the system by entering correct credentials and uploading the same image that was uploaded at the time of registration, if wrong credentials are entered then there will be login error and the same is for image. The server actually responses the client request as shown in Fig 5.1.the authenticated client can upload files into the storage and only authenticated client can access their own files

and if authenticated client tries to access other data in the storage then that client will be treated as intruder and will be blocked and a message will be sent to admin. The admin can login into the system by entering the correct credentials and the admin has the power to unblock the intruder.

Fig. 1: Architecture Diagram

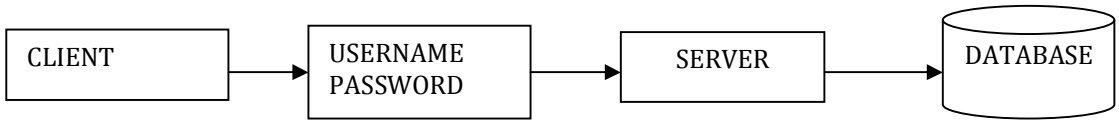


LOGIN MODULES

There are two login and one registration modules:
1. Client Login
2. Admin Login

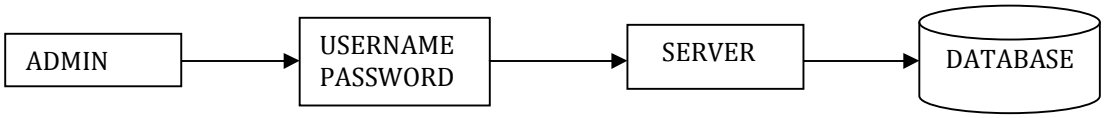
1. Client Login:
The client can login into the system by entering the correct username and password, the client first request the server then the server compares the client credentials in the database if they exists then the client can login into the system otherwise login error message will appear on the screen.

Fig. 2: Client Login



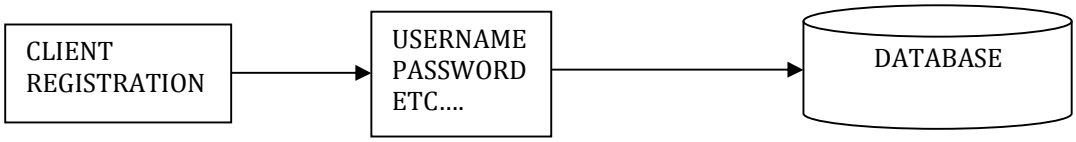
2. Admin Login:
The admin can login into the system by entering the correct username and password, the admin first request the server then the server compares the admin credentials in the database if they exists then the admin can login into the system otherwise login error message will appear on the screen.

Fig. 3: Admin Login



User Registration Module:
The client first needs to register by entering username, password etc. The clients credentials will be stored in the database.

Fig. 4: User Registration



The client will enter mail ID, city, state, phone number in the user registration form along with username and password.

EXPERIEMENTAL RESULTS

Fig. 5: Home Page (shows the home page it consists of client login, admin login and create new user options)

Fig. 6: New User Registration (shows how a user can register himself in a system by entering all the required fields)

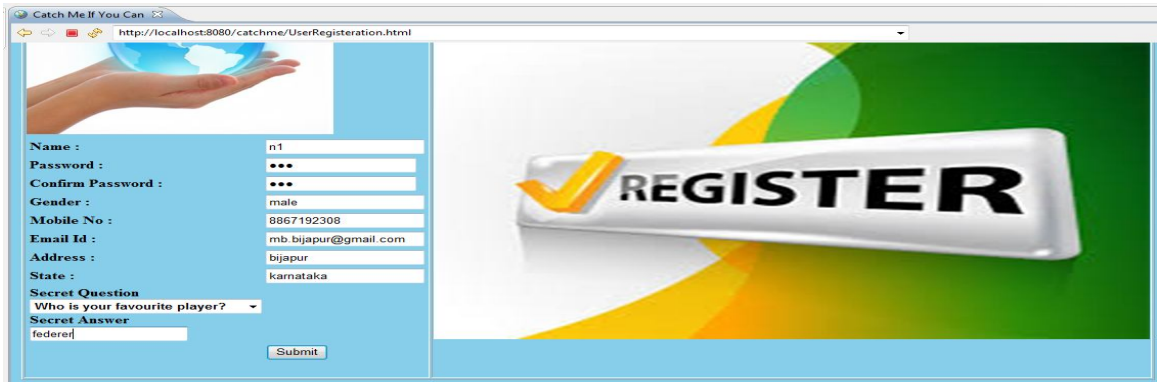


Fig. 7: User registered (shows all the details of the new user have been updated)

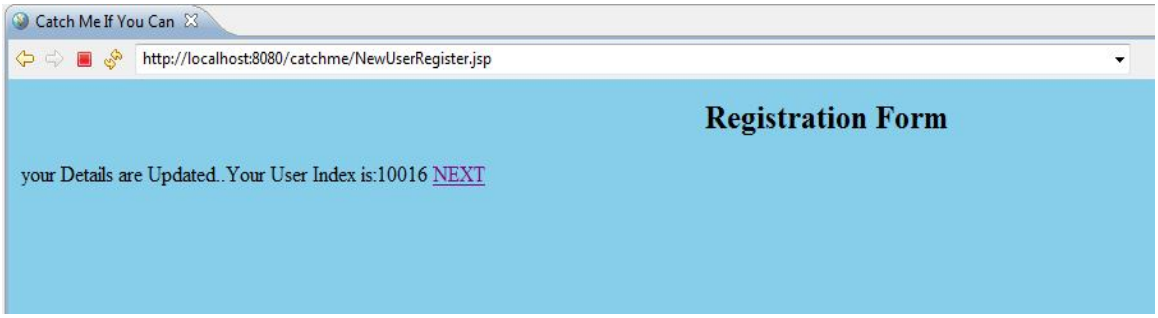


Fig. 8: Image Upload (shows how a user selects an image from the system at the time of registration)

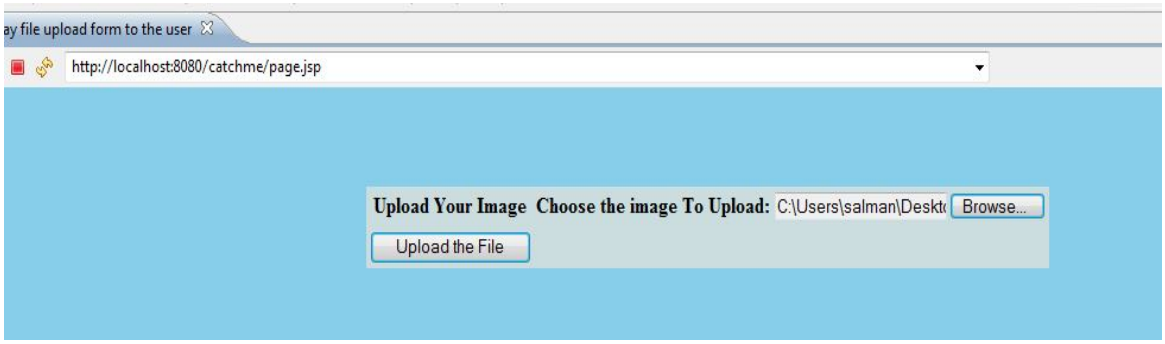


Fig. 9: Successful Image Uploaded (shows the snapshot of how the image was uploaded into the database successfully. BLOB is the data type used to store the image in the database)

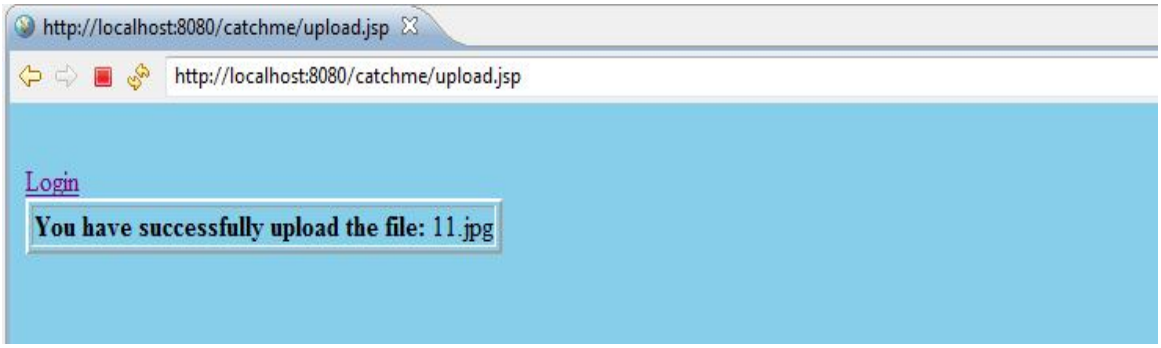


Fig. 10: Client Login (shows the client login page where a registered client can login using his/her credentials)

Fig. 11: Selecting the image to compare (shows graphical authentication technique, the client needs to select the same image that he/she uploaded at the time of registration; the system actually compares this with the image that was uploaded in the database at the time of registration)

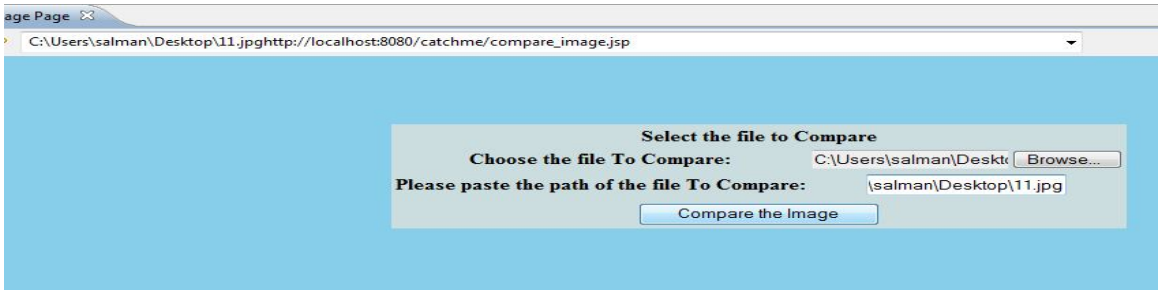


Fig. 12: Client Home Page (shows client home page where a client can upload any kind of file from the system)

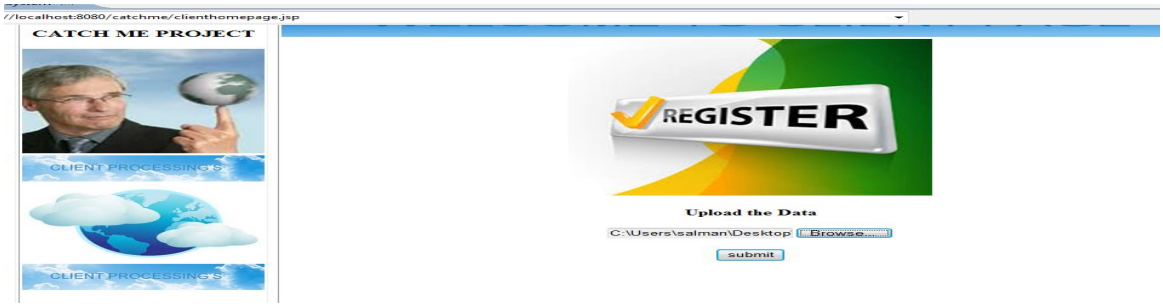


Fig. 13: Successful file upload (shows the client has successfully uploaded the file and only authenticated client can view the file)

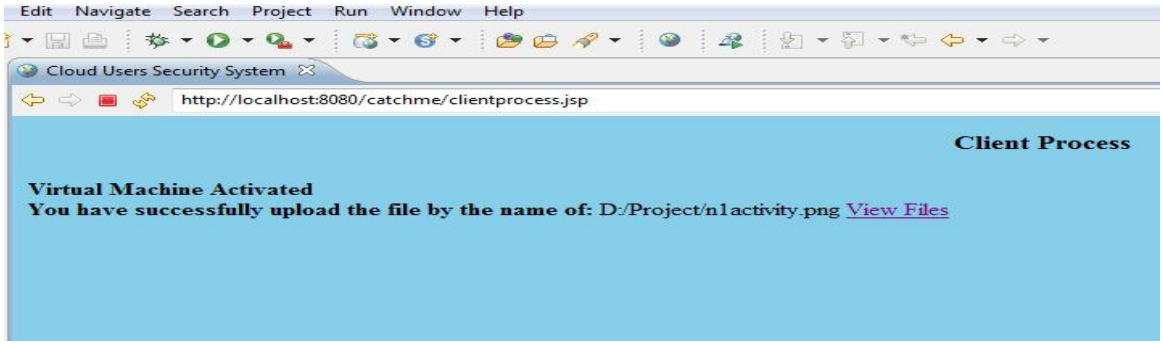


Fig. 14: User Uploaded Files (shows the storage which consists of files that user has uploaded and only authenticated user n1 can view his own file)

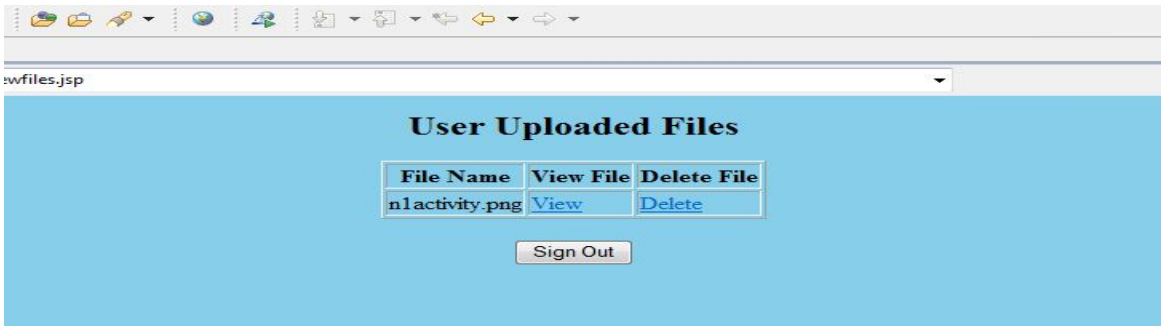


Fig. 15: Admin Login (shows the admin login page where admin enters his/her username and password and a randomly generated captcha, if admin enters any one of these wrongly then the login error message will appear on the screen)

Fig.16: Admin Home Page (shows admin can view all the user behavior)

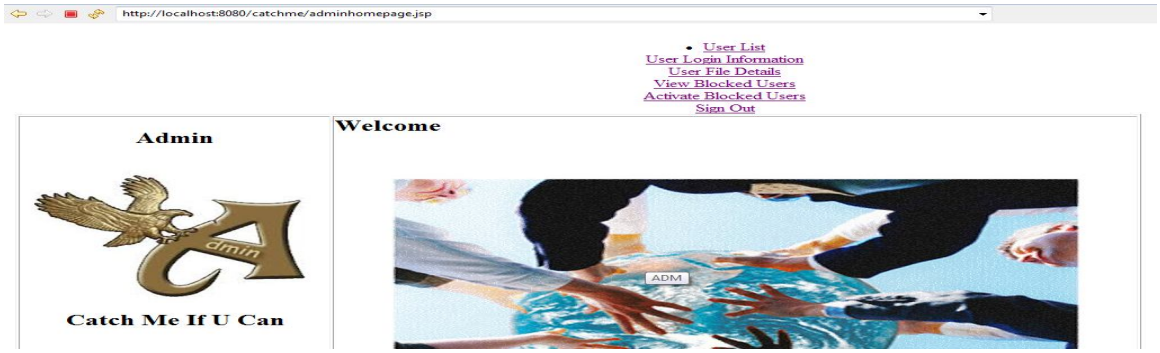
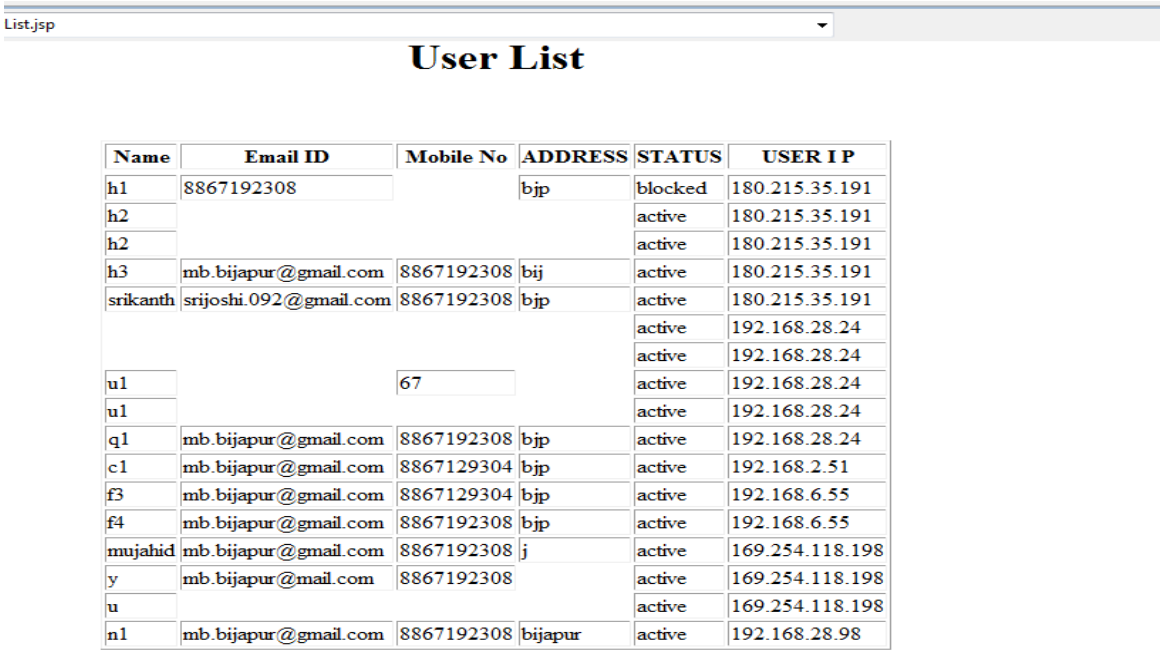


Fig. 17: User List (shows the list of users along with their information)



List.jsp

User List

Name	Email ID	Mobile No	ADDRESS	STATUS	USER I P
h1	8867192308		bjp	blocked	180.215.35.191
h2				active	180.215.35.191
h2				active	180.215.35.191
h3	mb.bijapur@gmail.com	8867192308	bij	active	180.215.35.191
srikanth	srijoshi.092@gmail.com	8867192308	bjp	active	180.215.35.191
				active	192.168.28.24
				active	192.168.28.24
u1		67		active	192.168.28.24
u1				active	192.168.28.24
q1	mb.bijapur@gmail.com	8867192308	bjp	active	192.168.28.24
c1	mb.bijapur@gmail.com	8867129304	bjp	active	192.168.2.51
f3	mb.bijapur@gmail.com	8867129304	bjp	active	192.168.6.55
f4	mb.bijapur@gmail.com	8867192308	bjp	active	192.168.6.55
mujahid	mb.bijapur@gmail.com	8867192308	j	active	169.254.118.198
y	mb.bijapur@mail.com	8867192308		active	169.254.118.198
u				active	169.254.118.198
n1	mb.bijapur@gmail.com	8867192308	bijapur	active	192.168.28.98

Fig.18: Blocked user page (shows admin can view the users that are blocked. Users are blocked if they try to access others data in the storage)

Fig.19: Activate user page (shows admin can activate the blocked user by entering the blocked user's name)

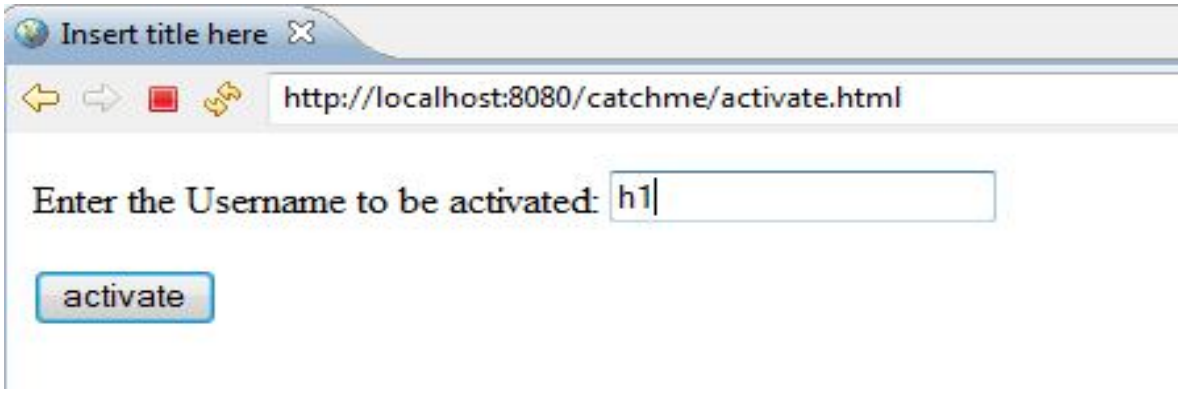


Fig. 20: User Files (shows the storage consisting of two users n1 and n2,now n2 can only view his own file the one in the docx format but n2 tried to access or view n1 file,so n2 will be treated as intruder and will be prevented from accessing n1 file)

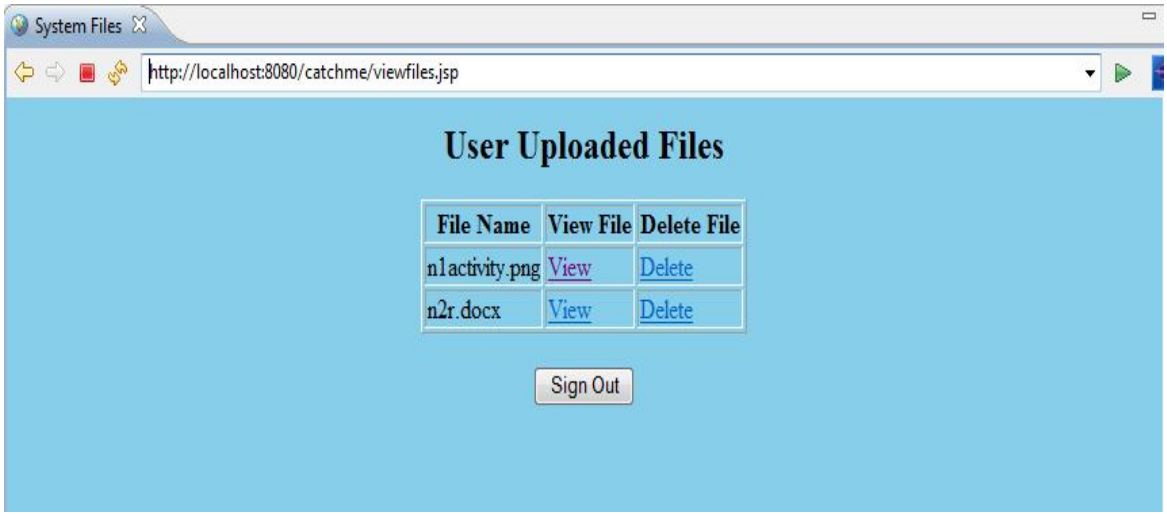
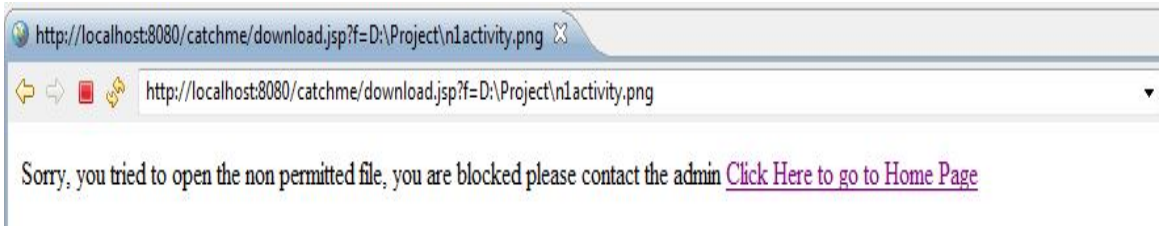


Fig. 21: Intrusion Prevention (shows intrusion prevention in the storage, the intruder is blocked and is left with message contact to admin)



CONCLUSION

Our proposed project work includes a common database for the clients/users where they can store the data and can have access to their own data. It also includes intrusion prevention technique and graphical user authentication technique. The proposed project work avoids unauthenticated client to access the data stored in the database or storage using the intrusion prevention and graphical user authentication technique.

1. Proposed project work avoids the unauthenticated client from accessing the data stored in the database.
2. It uses intrusion prevention technique for the above.
3. It also uses graphical user authentication technique as a second level of security for user authentication.
4. Intruder is blocked when accessing data stored by others in the database and is told to contact the administrator

REFERENCES

1. Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud (2005): Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 63:128–152.
2. Eugene H. Spafford (1992): Observing reusable password choices. In Proceedings of the 3rd Security Symposium. Usenix, pages 299–312.
3. G. E. Blonder (1996): Graphical passwords. *United States Patent, 5559961*.
4. G.E. Blonder (1995): Graphical password. U.S. Patent 5559961, Lucent Technologies, Inc. (Murray Hill,NJ), August 1995.
5. Gajbhiye S.K. and Ulhe P. (2012): Authentication Schemes for Session Passwords Using color and gray-scale images.
6. Harley Kozushko (2003): *Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems*.
7. L. Sobrado and J.C. Birget (2002): "Graphical Passwords", The Rutgers Schloar, An Electronic Bulletin for Undergraduate Research, vol 4.
8. Matt Carlson and Andrew Scharlott (2006): *Intrusion detection and prevention systems.*
9. Real User Corporation (2004): The science behind passfaces, June 2004.
10. Robert Morris and Ken Thompson (1979): Password security: a case history. Communications of the ACM, 22:594–597.
11. S.Balaji, Lakshmi.A, V.Revanth, M.Saragini, V.Venkateswara (2012): Reddy-Authentication Techniques for Engendering Session Passwords with Colors and Text.
12. Sigmund N. Porter (1982): A password extension for improved human factors. Computers & Security, 1(1):54– 56.
13. Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon (2005): Passpoints: design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies, 63:102–127, July 2005.
14. W. Jansen (2003): "Authenticating Users on Handheld Devices "in Proceedings of Canadian Information Technology Security Symposium.
15. William Stallings and Lawrie Brown (2008): Computer Security: Principle and Practices. Pearson Education.
16. Xiaoyuan Suo, Ying Zhu, and G. Scott Owen (2005): Graphical passwords: A survey. In Proceedings of Annual Computer Security Applications Conference, pages 463–472.