International Journal of Communication Networks and Information Security
2024, 16(4)
ISSN: 2073-607X,2076-0930
https://ijcnis.org/

Research Article

Web Based Graphical Password Authentication System

Raziya Begum[1], Gopalapuram Poojitha[2], Ramdas Vankdothu[3]

[1,3] Assistant Professor , Department of CSE, Balaji Institute of Technology & Science, Laknepally, Warangal
[2]M.Tech Student , Department of CSE, Balaji Institute of Technology & Science, Laknepally, Warangal
Corresponding Author : Ramdas Vankdothu(vramdas786sap@gmail.com)

ARTICLE INFO

Received: 17 Aug 2024
Accepted: 27 Sep 2024

ABSTRACT

In order to provide security and assurance, programs commonly make use of verification that is dependent on passwords. This is done for the aim of providing security. However, human behaviors, such as selecting terrible passwords and supplying passwords in square measurements, are considered to be "the most delicate association" in the verification chain. This is because human beings are the ones who are responsible for these activities. As an alternative to alphanumeric strings that are optional, it is feasible that consumers will select passwords that are either short or necessary in order to facilitate quick remember. Both of these options are available to them. The expansion of web applications and portable applications has made it possible for individuals to utilize these programs from a broad variety of devices at any time and from any location. This is possible because of the fact that these programs are portable. In spite of the fact that this new innovation provides an extraordinarily high level of simplicity, it also raises the possibility that a password could be divulged to bear riding attacks. An adversary can readily identify or use recording equipment that is positioned outside of the client's location in order to obtain the client's credentials. For the purpose of avoiding problems of this sort, it is essential for us to make use of an alternative method of confirmatory communication. Another method of authentication that can be applied in this situation is graphical authentication. The usage of the picture secret word is the most efficient approach for managing sign-on, which is less complicated than the process of memorizing and generating passwords that are basic. This method is the most effective method. The process of signing in can be completed by tapping the relevant places or performing the appropriate gestures over a picture that has been pre-selected. Both of these methods are acceptable.

1.INTRODUCTION

The connection that enables a device to validate the identification of a person who interacts with network resources is referred to as "client confirmation," and the phrase "client confirmation" pertains to this connection. When it comes to authentication, the most difficult type of authentication for all websites and applications is often a password that is written in a literary style. Whenever it comes to passwords, textual passwords are made up of a series of letters, numbers, and a variety of other special characters. It is feasible that consumers will use a single login and secret key for several records the majority of the time. This is something that can happen. The other side of the coin is that they are not completely achieved. Therefore, we ought to make use of passwords that include both capital and lowercase characters, as well as numerals and letters. This is because of the fact that this is the case. After that, at that precise point, these literary passwords are regarded as being enough capable of warding off assaults from the force of beasts. On the other hand, it is challenging to recall and thoroughly investigate a hidden word that is printed in a solid form. Customers are more likely to select passwords that are either brief or formed from a word reference than they are to select random sequences of letters and numbers. Customers are more likely to remember passwords that are brief, which is the reason behind this phenomenon. The weakest link in the authentication chain is said to be human behaviors, such as choosing weak passwords for new accounts and inputting weak passwords insecurely for subsequent logins. This is said to be the case because human activities are the most common cause of security breaches. Shoulder surfing is when someone glances over your shoulder to obtain crucial or confidential information, such as your secret phrase, ATM PIN, or Visa number, while you are inputting it into an electronic device. Shoulder surfing may be a very dangerous practice. When you surf the web using your shoulders, your privacy and safety are at risk. A robust password that is based on text is tough to remember and memorize because of the method involved. We are in the process of putting in place a robust graphical electronic validation framework that will safeguard consumers from being victims of shoulder riding assaults. This is being done with the intention of avoiding problems of this sort.

2.LITERATURE REVIEW

Wantong Zheng and Chunfu Jia were the ones who initially conceived of the notion of implementing a Consolidated PWD strategy. This system incorporates a component for verifying secret phrases that is known as integrated PWD. spaces) into the passwords in order to strengthen the framework that is already in place for validating secret words. For example, this system's use of separators allows it to accomplish this. The client's preexisting preferences are utilized in this method to its full potential. In accordance with this evaluation, users of the website have the possibility to incorporate spaces into their secret word at the point where they are required to stop when they register a record. Furthermore, the back-end of the website keeps a record of the amount of spaces that are present in each opening [1]. The client will build an underlying secret word in order to characterize the manner in which the secret key will be changing over the course of a specified amount of time, and we were able to discover that framework in the paper [2]. A one-time password email, a test, and a token device are some of the barriers that are connected with using a third party. This action was made in order to avoid these challenges and utilize a token device instead. After that, they made the significant discovery that the system keeps the robustness of the dynamic password while also making it simpler to use in terms of availability [2]. This was acrucial discovery.

Yang Jing Boo developed the concept of a trustworthy secret key validation layout. He was the one who came up with the idea. There are two sorts of one-time password authentication systems: weak password authentication schemes and strong password authentication schemes. Both of these techniques are vulnerable to being compromised. At the same time, each of these possesses both positive and negative aspects. Within the confines of this paper, we will present an outline of Kus's methodology, which will also demonstrate an assault on his convention. Furthermore, it was found that there are areas of strength for which there is a larger strength, and the possibility of successful speculation is unimaginable. This was discovered. Following that, we will present the areas of strength that will be utilized for a validation plot following this. In this work, the technique developed by W. C. Ku is built upon in order to make it possible for the change convention to withstand the assault that involves stolen verifier identification. Without sacrificing the effectiveness of the convention, the building of the modified convention has been successfully completed [3].

Within the context of this particular scenario, we employ the utilization of a picture password for the second authentication round. Because of this, there is no longer a requirement for complicated passwords that are also written down. Customers are free to utilize any fundamental written secret key, since this

provision allows for their usage. It is possible to break this system down into three distinct components. Location for work Additional reuse-arranged secret stage validation framework was proposed by Hua Wang and Yao Guo. This framework is known as the Secret key Verification Place (DPAC), and it was given the term DPAC. This framework's objective is to facilitate the reuse of countermeasures across applications, with the end goal of reducing the expenses associated with the protection of passwords from potential attacks. There is a possibility that this method may eliminate a considerable quantity of tedious work and bring about a reduction in expenses. We demonstrate the utility of DPAC by running a model in which we move the widely used OpenSSH to DPAC and carry out two model countermeasures [4]. In essence, this is how we demonstrate the helpfulness of DPAC. This is how we illustrate how DPAC can be applied in real-world situations.

The utilization of a secret phrase confirmation code, which is also referred to as a PAC in some instances, is a significant problem in a wide range of applications, such as websites, data set frameworks, and other applications that are otherwise comparable. The development of a PAC-RMPN approach takes place within the setting of Salah Re fish. A PAC that was built between two clients in order to authenticate confirmation between them is going to be presented in this article. The objective of this article is to present the PAC. This inquiry provides a fresh solution to the problem of secret word validation at the later level, which has been going on for a considerable length of time. The problem has been going on for quite some time. It would be prudent for them to design a strategy that would enable them to acquire this secret phrase from the ones who are intended to assault them. To generate a secret phrase for another client who needs to be confirmed, all that is required of a valid customer is to type his secret phrase and then hit the enter key. This is the only requirement that is necessary [5].

It has been suggested that a secure secret word verification plot be devised, which would result in an increase in the level of protected information. Included in this approach is the utilization of a combination of sham digits, key digits, and example digits. In order to accomplish this, the client needs to be able to detect and use design as network area numbers, register key characteristics that direct respect to the secret password, and attach faker characteristics in order to mislead the attacker. All of these capabilities are necessary in order to accomplish this. In order for the client to be able to log in, they must first check the example, and then they must lead the secret key from the design with the enrolled key attributes. One of the outcomes of this will be the production of a secret word that contains fictitious digits. Because to this method, the number of attacks that occur, including cross-site scripting, brute force attacks, shoulder surfing, and other types of attacks, is significantly reduced. because of the great intricacy of guessing passwords in multi-levels: first from the example, then, at that point, from key, and later from sham qualities [6]. The secret key is the most important key to obtain permission, but programmers are extremely skilled at breaking secret phrases since the customer chose a weak secret key. This is because the secret key is the most important key to receive permission. The proposed system makes use of the Honeyword approach, which is closely connected to Honey encryption, in order to construct the mystery key store. Honey encryption is strongly related to Honeyword. Honeywords contain bogus passwords that are used in conjunction with a one-of-a-kind mystery word in order to catch the attention of the person who is attempting to breach the system. As the name suggests, Honeyword is a program that incorporates passwords that are intended to be deceiving. This is the program's fundamental principle. There is a deliberate intention that these will result in an assault. From the perspective of the methodology that is now in use, there are a variety of various approaches that can be applied in order to generate the Honeyword of a one-of-a-kind secret phrase. Some examples of these tactics are the Teasing with-tweaking model, the Teasing with-secret phrase model, and others that are similar to these [7].

3.PROPOSED SYSTEM

1. The purpose of this part is to work on the development of an electronic application that takes use of graphical validation. It is utilized that there are two unique layers of security.

The modules that make up the Graphical Secret Key Framework of the Framework Public Module, Number Three are the ones shown in Figure 1.

Four. This brings us to the end of the comprehensive review that was conducted for a single website. This particular module is available to everyone who has the URL entered into their browser. In spite of the fact that the information is accessible to the general public, they are unable to modify or update it. The adaptability of the client

6. The customers who have signed up for the client module are the units that make up the client module. Both the registration and the login capabilities are included in the user module. These are the two features that it consists of. During the enrollment process, the framework is responsible for gathering the fundamental information about the client. Personal information such as the client's name, cell phone

number, email address, printed secret phrase, and graphical concealed phrase are included in this information. In the data gathering, each and every one of them is mixed up and accounted for in a separate location. In order to acquire access to the resource, the user will be asked to provide the username, the textual password, and the image password during the login stage. This is necessary in order to gain admission to the resource. During the process of registering for the service, it makes a comparison between the values that have been provided and the information that the user supplies throughout the procedure. When it is determined that it is a match, the individual in question will be logged in to the page.

Configuration Settings and Recording Instructions

This is the third module, and it contains the client's records as well as the numerous settings of the updated web stage. It is the eighth module. By establishing a connection between the client module and the record module, it is feasible to accomplish this. In the event that the customer successfully completes the enrollment procedure, the record will be added to the data collection. Customers also have the flexibility to change their passwords whenever they want, which is an additional convenient feature. Considerations pertaining to protection and security, information concerning sign-in, and other similar matters are among the advantages that it offers. This part also provides customers with the opportunity to obtain admonitions and support for solicitation of their business.

4.SYSTEM ARCHITECTURE

On the basis of the design, a determination is made concerning the usefulness of the building. The architecture of the web application reflects a number of various skills, including the ability to manage a large number of solicitations, the time it takes to respond to requests, and the amount of time it takes to stack pages. The execution of the project will therefore be improved as a result of the implementation of the design that can be considered the most effective. In this particular situation, MVC engineering, which is also commonly referred to as Model-View-Control Design, is applied. Model-View-Regulator design, which is a model design strategy for programming projects, is something that MVC Engineering suggests building. This design is a model design strategy. Figure 3 illustrates the three components that comprise the plan, which are referred to as the Model, View, and Regulator. As a result of these components, the framework has been enhanced in terms of its adaptability.

It is the responsibility of the Model layer, which is the most fundamental layer, to deal with the associations that exist between the various data sources and information. As the layer that displays the results or acts as the review layer in an MVC architecture, the View layer is the layer that is responsible for this. The Regulator is responsible for selecting the information stream, and one of the functions that it plays is that of a mediator between the model and view components. This component is also responsible for selecting the information stream. The result of this is that it passes the data that belongs to the client via the Model segments in an iterative manner before transferring it to the View segment. The System's Architecture and Design When the user reaches the client's border, they begin the process of requesting registration service. There are two distinct encryptions that are applied throughout the length of the registration procedure. The first one, which has the secret phrase in text, and the second one, which contains the secret phrase in graphic form. As a direct consequence of this, the Graph Pass section was cut into four separate slices. The encryption process is carried out on each individual slice. The implementation of graphical user interfaces that are easy to understand makes the task significantly less difficult. In a similar manner, the customer does not need to be concerned with understanding the programming language or their own way of thinking.

In order to ensure that it is in complete accordance with the Model view regulator plan (MVC engineering) standard, the framework has been created precisely in this manner. The Model-View-Regulator design system, which is also commonly referred to as MVC Engineering, is a model design technique that was developed expressly for the purpose of programming projects. In this particular situation, we make use of the SQL laborer in order to store all of the client data. This is in addition to the fact that it necessitates the utilization of a more robust data set that is able to hold a substantial amount of data. It is the responsibility of the web-based application in issue to ensure that the client-server architecture is successfully maintained. There will be a number of different devices connected to the client side, and these devices will communicate with the server by utilizing the web and the cloud. The client side will be connected to the various devices. Whenever a client delivers a request to the server, the server responds by delivering the information that is pertinent to the request that was delivered by the client. Customer-Server Architecture is a form of processing paradigm in which the worker owns, transports, and manages the majority of the assets and services that the customer will use. This style of architecture is also

known as Client-Server Architecture. There is another name for this approach, which is a client-server architecture. This type of design is comprised of at least one client laptop that is linked to a server by either a network connection or a web connection. Sharing of figurative assets is accomplished through the utilization of this framework. As a result of the fact that all of the sales and organizations are distributed throughout an association, the client/server design is frequently referred to as the organization handling model of a framework or the client/specialist network.

Structure of the Framework's Architecture

With regard to the client side of things, the PHP framework that we make use of is known by the name CodeIgniter. The architecture that it is a part of is known as MVC, which is an acronym that stands for Model View Control. When the model session is in progress, the database operations are being handled and arranged.

Activities such as database comparisons and validations are carried out during the session that has been designated for the model. In the course of the control session, the functions that are of a general nature are carried out.

5.IMPLEMENTATION

Each of the following instruments was utilized in the execution of the implementation: Devices and software .Within the context of this particular development, the text editor known as Sublime Text is utilized. Shareware distribution is provided for Brilliant Text, which is a source code manager that supports multiple stages. A connection point for the Python application programming language, which is often referred to as a computer programming interface, is included in this product. Users have the opportunity to add functionality to their apps by utilizing plugins, and native support is offered for a broad number of programming languages and markup languages. Additionally, users have the ability to add functionality to their applications. In most cases, these plugins are produced locally and maintained under licenses that are made available for free software. A successful completion of the server configuration was achieved through the employment of XAMPP. Apache Companions is the organization that is responsible for the development of XAMPP, which is a web server architecture stack package that is open-source and free. ExAMPP is designed to work across multiple platforms. The Apache HTTP Server, the MariaDB data store, and mediators for scripts written in the PHP and Perl programming languages are the primary components that make up this system. As a result of the fact that the majority of actual web server installations make use of the same components as XAMPP, it is not difficult to migrate from a local test server to a live server. This is made possible by the fact that the vast majority of web server deployments make use of the XAMPP content management system.

For Structured Query Language, SQL is an acronym that stands for the full phrase. Its purpose is to make collaboration with data collection methods easier to do. There is the possibility that it might be applied for the purposes of storing data from databases, managing that data, and retrieving that data using it.

Instruments and apparatuses

The hardware requirements for this task include a CPU with an i3 or higher processor, a random-access memory (RAM) capacity of at least 4 gigabytes, and a solid-state drive (SSD) capacity of at least 2 gigabytes.

6 RESULT

A representation of the graphical password authenticator can be seen in the image that can be found above. At the conclusion of the enrollment procedure that takes place on this landing page, the customer will be able to view his or her profile. When it comes to security, the Enlistment area is equipped with two different levels of protection. A literary secret key and a graphical secret key are the two types of secret keys that are included in this group.

It is possible for a customer to access their profile by clicking the login button that is located on the home screen. There are two extra layers of protection that are included on the login screen, as was described earlier in the statement that came before this one.

When it comes to this project, we are utilizing images as a means of verifying the identities of users. The user will be needed to click on these images four times in order to select four separate locations of their choosing, which they will need to remember. These photographs will be uploaded throughout the process of signing up for the service.

Due to the fact that it is impossible for users to determine the precise pixel X and Y location from a mouse click, we provide authentication that is dependent on the region. In the situation that a user selects X = 120 and Y = 240, for instance, I will deduct 10 pixels from the X value and add 10 more pixels to the X values in order to finish the authentication process. This is done in order to ensure that everyone is

authenticated. The user will be officially acknowledged as the real or authentic version if they select an X number that falls between 110 and 130 and a Y value that falls between 230 and 250. In other words, if they choose these values, they will be able to use the X number. This module allows administrators to log in to the application by using their username and secret key in order to access the application. This module is implemented so that administrators can access the application. Administrators are able to examine all of the client details that have been enlisted within the system once they have successfully signed in.

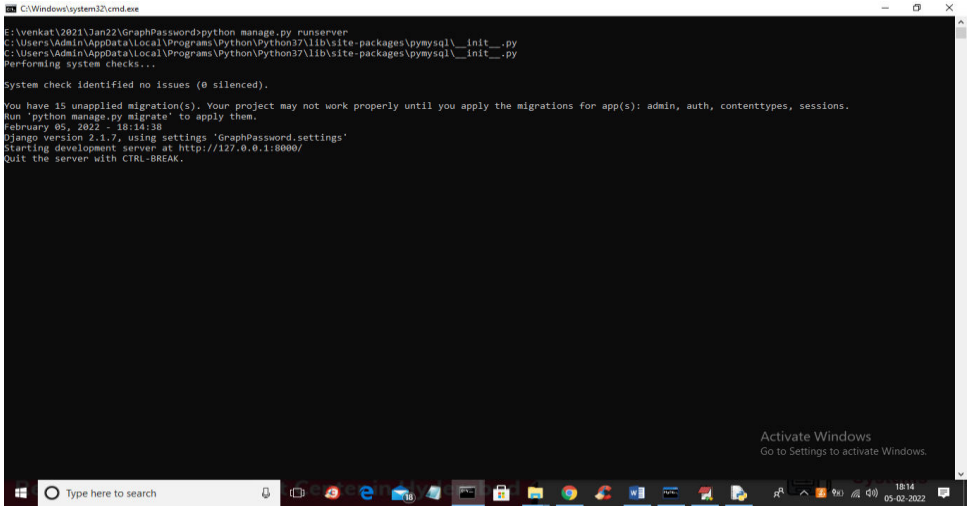
2) New Client Information Exchange: The client is able to communicate with the application. This module allows the client to exchange information with the application. Instead of sending a secret phrase, the client is asked to transmit an image. After that, they must choose four locations, and the information that they provide will be captured and stored in the data set.

User Login is the third module, and it allows users to log in to the application by entering their username. This module is included in the application. After that, an image will be displayed, and in order for the user to be authenticated, they will be asked to select the relevant locations on the image.

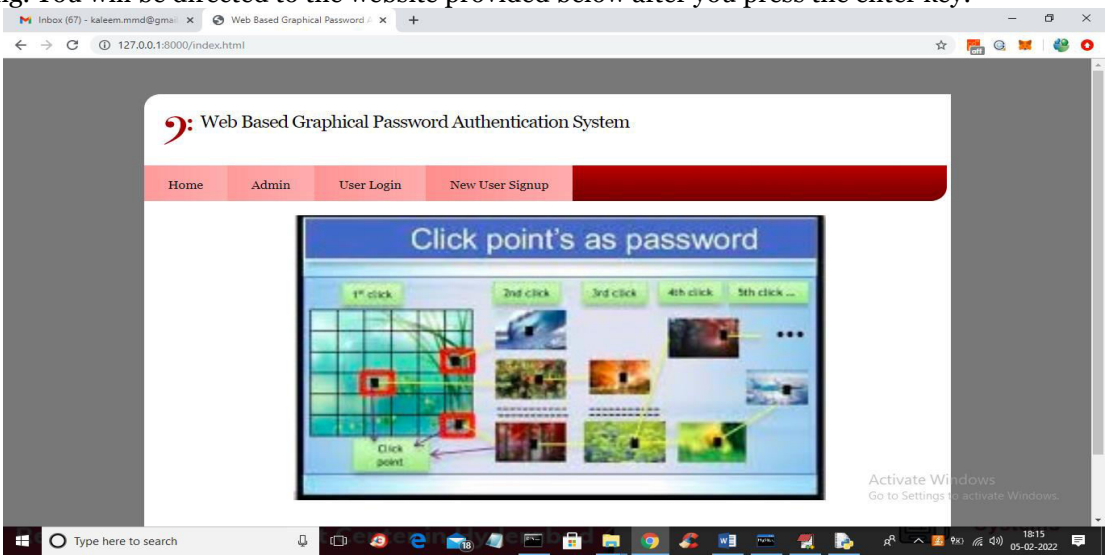
4) Reset Secret Key: Once the customer has successfully signed in, they have the ability to refresh the secret key picture and add new locations in order to reset the secret key.

7 SCREEN SHOTS

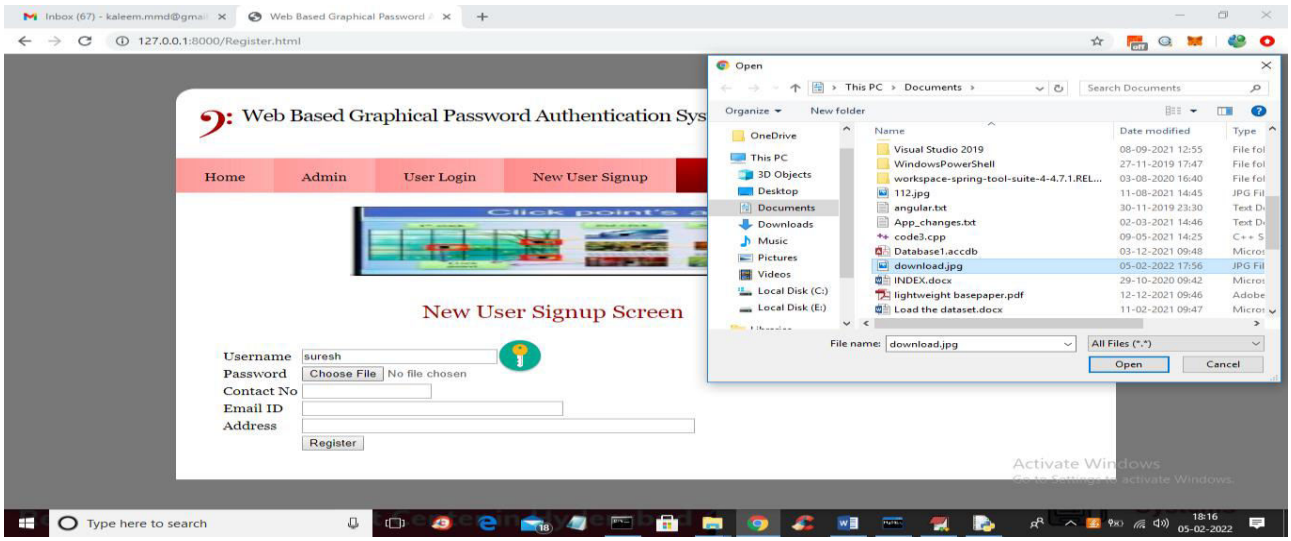
Initiate the DJANGO server by double-clicking the 'run.bat' file, as demonstrated on the screen below, to run the project.



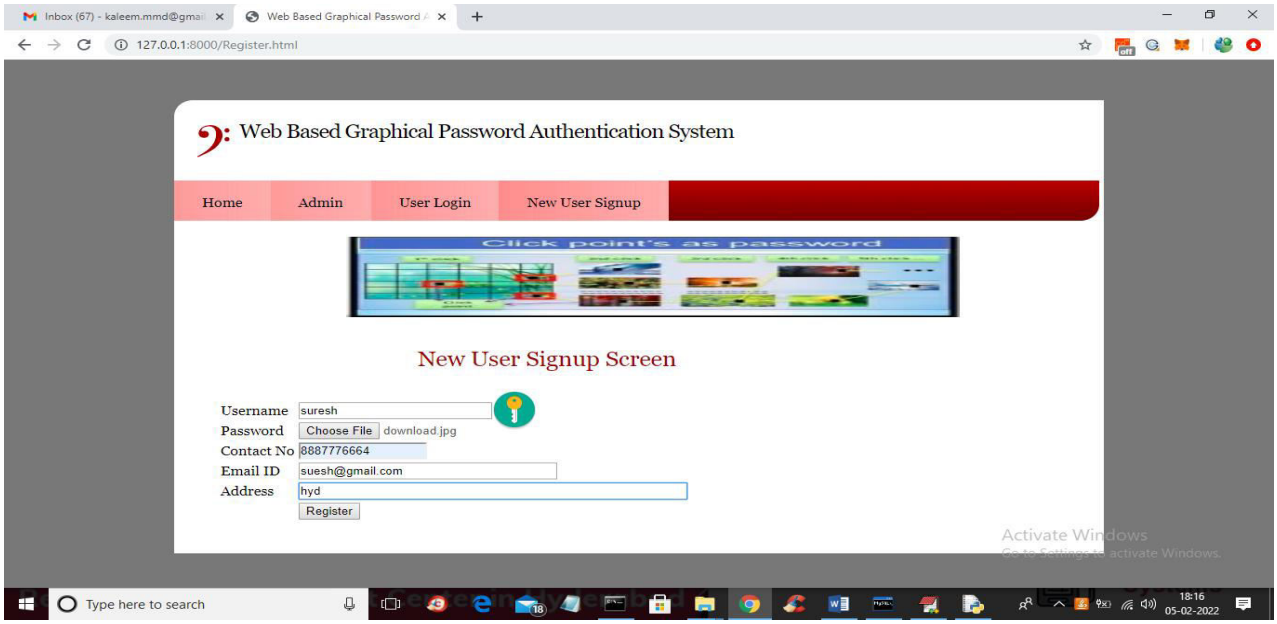
Launch a web browser and type in http://127.0.0.1:8000/index.html; the DJANGO server is now up and running. You will be directed to the website provided below after you press the enter key.



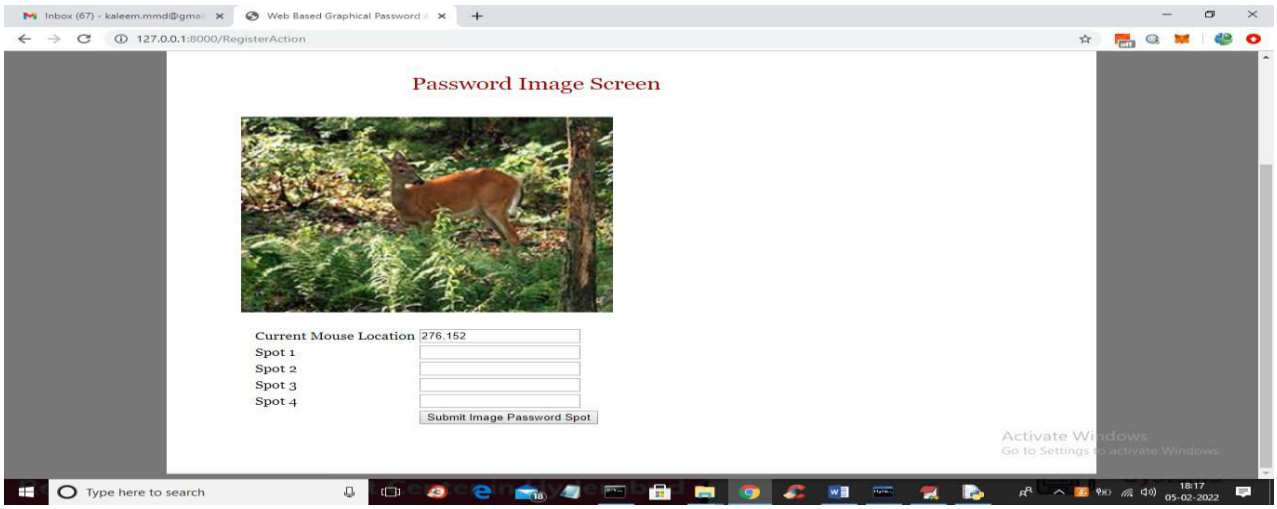
The 'New User Signup' link may be seen on the screen above; to input new user details, click on it.



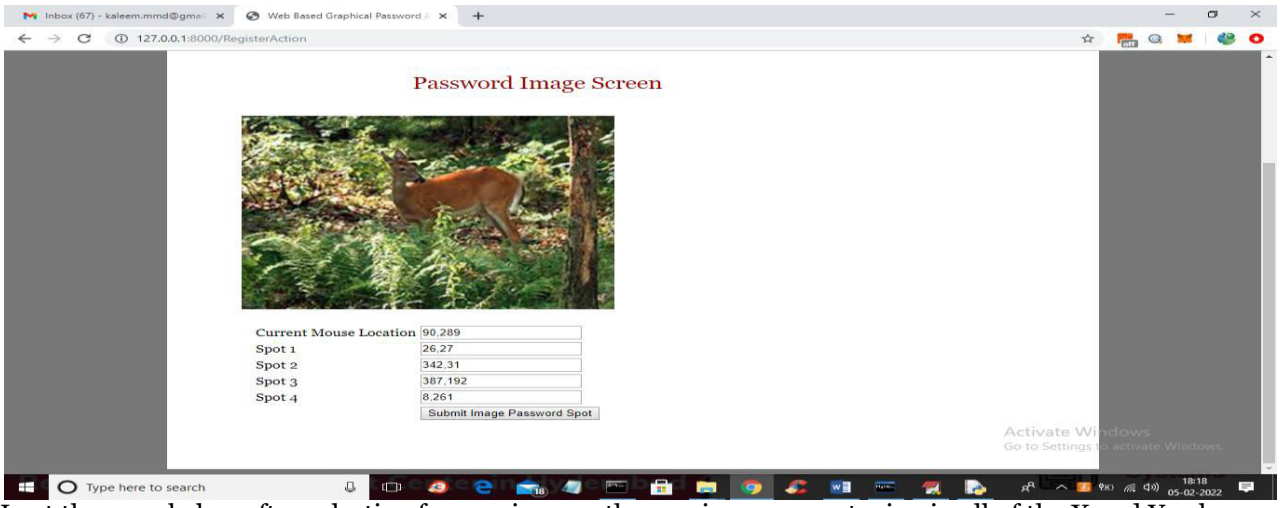
The user is providing their signup details on the screen seen above, but instead of inputting a password, they are browsing the web and uploading an image. They will then input the remaining data.



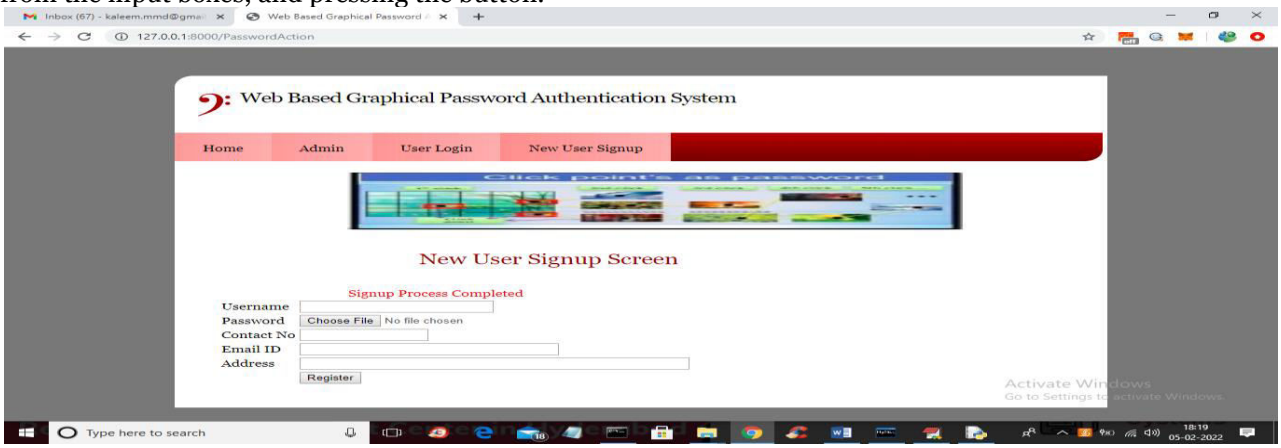
After you've done filling out all the necessary fields, click the "Register" button up there to bring up the image below.



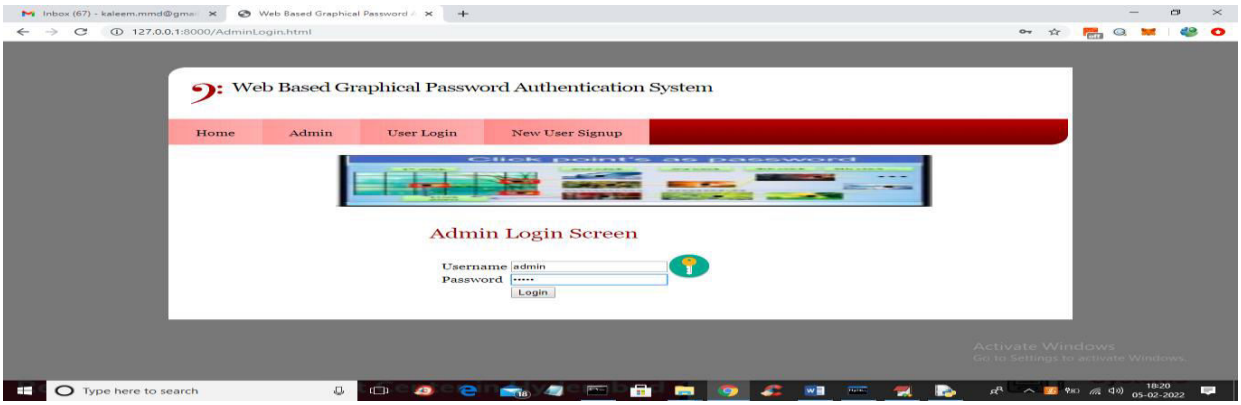
To add a place to the text fields, the user needs to click on any part of the region depicted in the image above. If you want to know where your mouse is right now, you can see its current location in the first field. Afterwards, you'll be taken to the screen below after you've chosen four positions.



I got the page below after selecting four regions on the previous screen, typing in all of the X and Y values from the input boxes, and pressing the button.

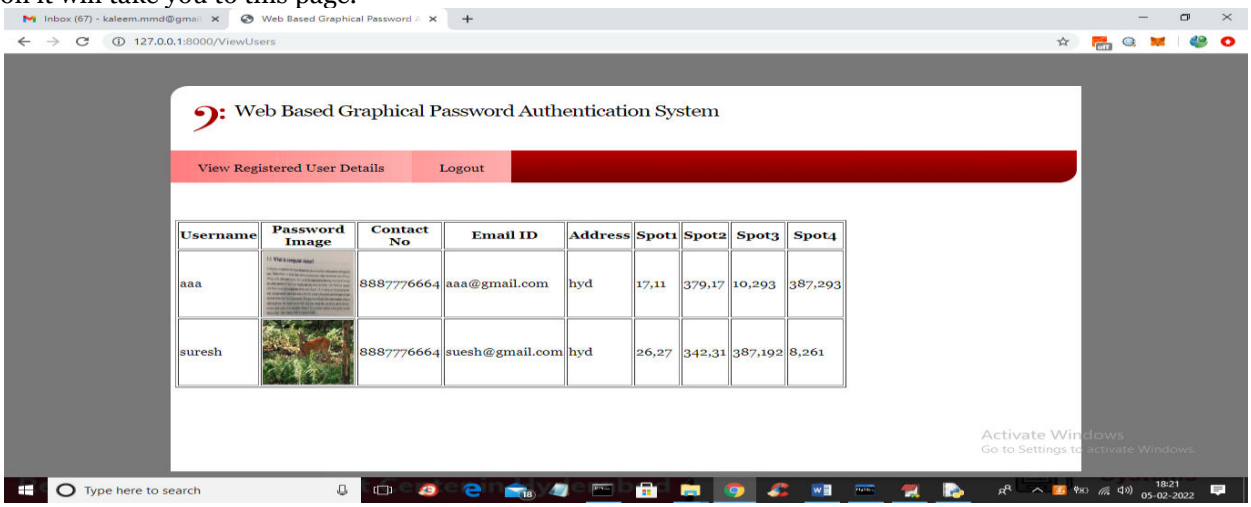


To view all of the user details as an administrator, please click on the 'Admin' option that appears. On the screen just above us, a notification stating "signup process completed" appeared.



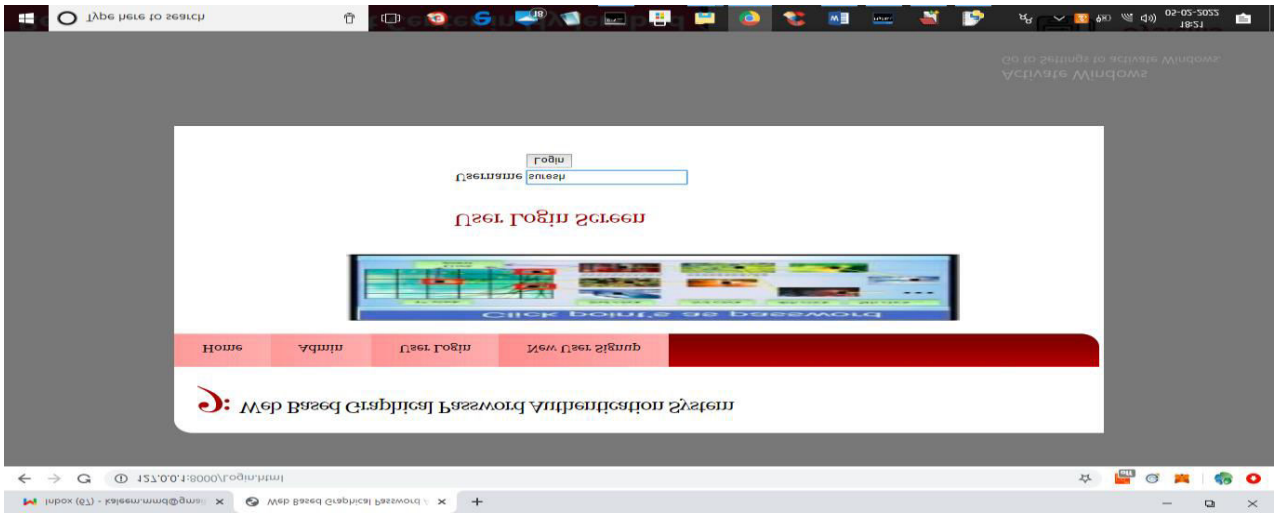
The following screen will be shown to the administrator after they have successfully logged in.

In the screen that appears above, you can find the link that reads "View Registered User Details"; clicking on it will take you to this page.

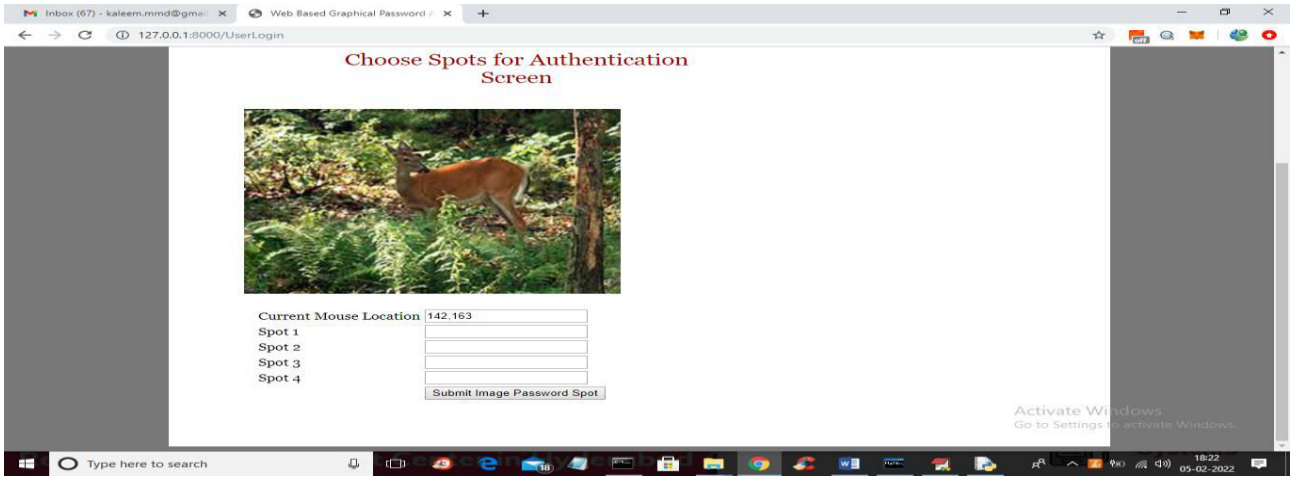


Username	Password Image	Contact No	Email ID	Address	Spot1	Spot2	Spot3	Spot4
aaa		8887776664	aaa@gmail.com	hyd	17,11	379,17	10,293	387,293
suresh		8887776664	suesh@gmail.com	hyd	26,27	342,31	387,192	8,261

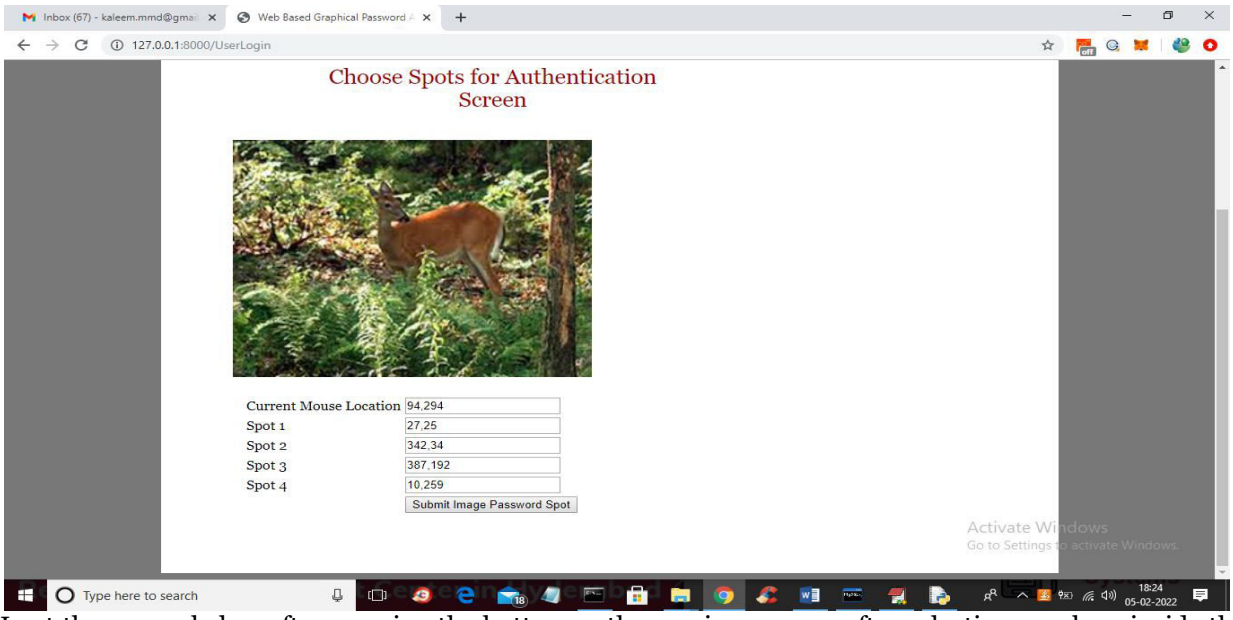
The graphic up there shows all the user info that admins can see, including passwords and usernames. In addition to being able to log out and back in as Suresh, they now have the option to select four different places.



After entering their username and password on the login screen, users can access images and choose among locations that look like the ones below by pressing a button.



A user must also authenticate himself by clicking the button after selecting four places on the screen shown above.



I got the screen below after pressing the button on the previous screen after selecting numbers inside the range. The user would be authenticated and shown the screen below if the provided locations happened to be within the correct database password points.

The success of the login process is indicated by the red lettering on the screen. The authentication process is susceptible to failure in the event that you supply erroneous information. To change your password to one that is more secure and allows you to choose different images and places, follow the steps outlined above by clicking the "Rest Password" link.

Be advised that in order to display new spot values, it is just necessary to remove any existing values from any field.

8. CONCLUSION

Customers must verify themselves each time they want to access their records and information. This is to ensure that their private electronic property is protected. You run the risk of shoulder riding assaults if you're in charge of the confirmation cycle all day long. When using the traditional methods of authentication, such as personal identification numbers (PINs) or normal textual passwords, users are prompted to enter their passwords. Because of this, these passwords are easy to crack using technologies that capture video, such as mobile phones, or by just looking over someone's shoulder. We proposed a confirmation architecture that accounts for graphical passwords and is secure for shoulder surfing to address this issue.

REFERENCES

[1] Zheng Wantong, Jia Chunfu, and the GroupPWD: A Novel Method for Password Authentication That Makes Use of Spaces Between Keystrokes: Presented at the 2017 Thirteenth International Conference on Computational Intelligence and Security (CIS)

[2] "User Define Time Based Change Pattern Dynamic Password Authentication Scheme," handed in by Salisu Ibrahim Yusuf and Moussa Mahamat Boukar in 2018, at the 14th International Conference on Electronics and Computers.
[3] At the 2010 Conference on Software Technology and Engineering, Second International Conference, Shen Pingping, Yang Jingbo, and Yang Jingbo presented an authentication system that is both secure and strong for passwords. presented by Hua Wang, Yao Guo, and Xiangqun Chen at the 2008
[4] IEEE High Assurance Systems Engineering Symposium: DPAC: A Reuse-Oriented Password Authentication Framework for Improving Password Security
At the 2018 International Conference on Advanced Science and Engineering (ICOASE), Salah Refish presented PAC-RMPN, which stands for Password Authentication Code Based RMPN.
[5] Ramdas Vankdothu, Dr.Mohd Abdul Hameed "A Security Applicable with Deep Learning Algorithm for Big Data Analysis",Test Engineering & Management Journal,January-February 2020
[6] Ramdas Vankdothu, G. Shyama Chandra Prasad " A Study on Privacy Applicable Deep Learning Schemes for Big Data" Complexity International Journal, Volume 23, Issue 2, July-August 2019
[7] Ramdas Vankdothu, Dr.Mohd Abdul Hameed, Husnah Fatima " Brain Image Recognition using Internet of Medical Things based Support Value based Adaptive Deep Neural Network" The International journal of analytical and experimental modal analysis, Volume XII, Issue IV, April/2020
[8] Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima" Adaptive Features Selection and EDNN based Brain Image Recognition In Internet Of Medical Things " Journal of Engineering Sciences, Vol 11,Issue 4 , April/ 2020(UGC Care Journal)
[9] Ramdas Vankdothu, Dr.Mohd Abdul Hameed " Implementation of a Privacy based Deep Learning Algorithm for Big Data Analytics", Complexity International Journal , Volume 24, Issue 01, Jan 2020
[10]Ramdas Vankdothu, G. Shyama Chandra Prasad" A Survey On Big Data Analytics: Challenges, Open Research Issues and Tools" International Journal For Innovative Engineering and Management Research,Vol 08 Issue08, Aug 2019
[11] Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima" A Brain Tumor Identification and Classification Using Deep Learning based on CNN-LSTM Method" Computers and Electrical Engineering , 101 (2022) 107960
[12] Ramdas Vankdothu,.Mohd Abdul Hameed "Adaptive features selection and EDNN based brain image recognition on the internet of medical things", Computers and Electrical Engineering , 103 (2022) 108338.
[13]Ramdas Vankdothu,.Mohd Abdul Hameed,Ayesha Ameen,Raheem,Unnisa " Brain image identification and classification on Internet of Medical Things in healthcare system using support value based deep neural network" Computers and Electrical Engineering,102(2022) 108196.
[14]Ramdas Vankdothu,.Mohd Abdul Hameed" Brain tumor segmentation of MR images using SVM and fuzzy classifier in machine learning" Measurement: Sensors Journal,Volume 24, 2022, 100440 .
[15]Ramdas Vankdothu,.Mohd Abdul Hameed" Brain tumor MRI images identification and classification based on the recurrent convolutional neural network" Measurement: Sensors Journal,Volume 24, 2022, 100412 .
[16]Bhukya Madhu, M.Venu Gopala Chari, Ramdas Vankdothu,.Arun Kumar Silivery,Veerender Aerranagula " Intrusion detection models for IOT networks via deep learning approaches " Measurement: Sensors Journal,Volume 25, 2022, 100641
[17]Mohd Thousif Ahemad ,Mohd Abdul Hameed, Ramdas Vankdothu" COVID-19 detection and classification for machine learning methods using human genomic data" Measurement: Sensors Journal,Volume 24, 2022, 100537
[18]S. Rakesh [a], NagaratnaP. Hegde [b], M. VenuGopalachari [c], D. Jayaram [c], Bhukya Madhu [d], MohdAb dul Hameed [a], Ramdas Vankdothu [e], L.K. Suresh Kumar "Moving object detection using modified GMM based background subtraction" Measurement: Sensors ,Journal,Volume 30, 2023, 100898
[19]Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Efficient Detection of Brain Tumor Using Unsupervised Modified Deep Belief Network in Big Data" Journal of Adv Research in Dynamical & Control Systems, Vol. 12, 2020.
[20] Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Internet of Medical Things of

Brain Image Recognition Algorithm and High Performance Computing by Convolutional Neural Network" International Journal of Advanced Science and Technology, Vol. 29, No. 6, (2020), pp. 2875 – 2881

[21] Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Convolutional Neural Network-Based Brain Image Recognition Algorithm And High-Performance Computing", Journal Of Critical Reviews,Vol 7, Issue 08, 2020(Scopus Indexed)

Mrs.Raziya Begum working as Senior Assistant Professor in the Department of Computer Science and Engineering ,Balaji Institute of Technology and Science , Telangana from 2007 to Till Date .Currently pursuing PhD in the stream of **"Data Science (Machine Learning)"** at **Koneru Lakshmaiah EducationFoundation** (KLEF), is a higher educational institution Deemed to be University, located in Vaddeswaram near Vijayawada, Andhra Pradesh, India.. She published more than papers in reputed Journals, attended nearly 3 International Conferences, attended nearly 20 faculty development programs, workshops and webinars ,1 patent. She is the Life Member in Professional Bodies IAENG.

Gopalapuram Poojitha pursuing Post Graduation in Balaji institute of technology and science,Laknepally,Telangana and completed Graduation in computer science ,Balaji Institute of Technology and Science,Telangana .She is working as Project Engineer,Wipro Limited.