Journal of Advanced Zoology

ISSN: 0253-7214

Volume 44 Issue -3 Year 2023 Page 1436:1448

DESIGN AND IMPLEMENTATION OF A SERVER INDEPENDENT THREE LEVEL AUTHENTICATION SYSTEM

[1]K. Nirmala, [2]Dr. N. Usha Rani

[1]Research Scholar, Department of Computer Science and Engineering, Sri Venkateswara College of Engineering, Tirupati, A.P, India

[2]Associate Professor, Department of Computer Science and Engineering, Sri Venkateswara College of Engineering, Tirupati, A.P, India

Article History
Received: 12 Aug 2023
Revised: 10 Sept 2023
Accepted: 29 Sept 2023

ABSTRACT: As the rapid growth of Internet of Things (IoT) technology in the healthcare sector has led to the emergence of many security threats and risks, the increasing use of sensor objects in the medical field has become quite challenging to ensure full protection. Security and Privacy are among the vital requirements for the IoT (Internet of Things) network domain, which involve data authentication and security. There are numerous approaches to arrange authentication and authorization within information systems. Usually, authentication is utilized for login purposes and essentially acts as a security tool for personal user data. It represents the first level of protection against the disclosure of any system information. Users no longer trust traditional password-based authentication methods, given the increased interaction among online services. Credentials acquired online are frequently utilized to secure additional credentials, and advanced attacks frequently focus on the least secure among a large number of available credentials. One-time passwords and a two-factor authentication mechanism are being investigated by researchers as they seem to present a natural progression from traditional username/password schemes. Authentication is one of the primary ways of establishing and ensuring security in the network. Hence in this work, design and implementation of a server independent three level authentication system is presented. In this system, three levels of authentication such as face recognition, matrix recognition, email and OTP (One Time Password) verification. After successful three level authentications, Hospital Management/administration can access the medical data. This system performs three level authentications which is unique and novel as a result intruder is not able to steal the medical information. Hence, this system will provide greater security.

KEYWORDS: Security, Privacy, Authentication and Three level authentication system.

I. INTRODUCTION

The advancement of technology has resulted in the growth of the Internet, which has influenced different aspects of our daily lives. In the last two decades, the way humans access public services, travel booking services, e-learning, banking services, and more has been revolutionized, with a significant increase in the utilization of web-based systems. Web services are an emerging technology in the web era, where service providers can describe and publish web methods, which can then be accessed by other service requesters or web programs using the internet. With the rise of web services technology, flexibility and vitality are becoming the core characteristics of inter-organizational business processes, including distributed auction services, business process integration, and order processing [3].

In the information age, new technologies are continuously emerging, fundamentally changing the way we study and work, including big data, cloud computing, and wireless sensors. However, data security has become an issue. Security, in general, refers to the state of being protected against losses or dangers. Security and safety are closely related concepts. While the word 'security' is synonymous with 'safety,' in technical terms, 'security' implies not only being secure but also having been secured. Hence, security can be described as "the quality or condition of having been protected to ensure freedom from danger."

In today's world, an increasing amount of sensitive data is being stored and processed by computer systems. Thus, there is a growing need to enhance the security of these systems to protect important data. Security involves the authorization of access to information under the control of the network administrator. The objective of ensuring network security is not only to ensure the security of the end system but also that of the entire network.

In the present digital era, the motivation for securing computing systems has changed. In a diversified environment, the traditional approach is to secure computing systems, servers, and conducting reliable audits does not provide a complete level of security for communication transactions. Whether the services or applications they are accessing are safe or not is determined by the users. Hence, safety and security is one of the prime design factors for robust security encouraging developers to ensure higher safety in web-based services. Over the years, computing resources have transitioned from a centralized system to a distributed one, and more commonly, to a cloud-based virtual centralization [7].

The process of authentication involves determining if a user or process is the entity or person it claims to be, thereby verifying the communicating entity is authentic. During the authentication process, the user is required to provide the necessary credentials for accessing the web service [1]. Authentication is utilized by a server when it needs to precisely establish who is accessing its information or website. A client utilizes authentication when it requires confirmation that the server is the system it claims to be [8].

Authentication involves the requirement for the computer or user to demonstrate its identity to the client or server. Typically, server-side authentication involves the utilization of a username and password. Alternative authentication methods include cards, voice recognition, retina scans, and fingerprints. When it comes to client authentication, it typically entails the server providing a certificate to the client, establishing trust through a trusted third party, such as the entity (like a bank) that the client expects the server to be associated with. Authentication does not determine what kind of tasks the individual can do or which files the individual can see. It only identifies and verifies who is accessing the server, whether a system or a person [2].

Common methods to break the current authentication system, including password dictionary, brute force attack, etc. Most of the current systems only have one-layer protection which is password for online systems. The security of information and communication systems is designed to protect information within systems used for searching, processing, and storing information. These systems encompass control systems for various application programs, devices, and databases, etc. Furthermore, it also extends to computer systems designed for disseminating information, including wireless and local control networks, the Internet, satellite communications, radio communications, and mobile communications, etc. This security aims to protect against unauthorized access, destruction, and counterfeiting.

To prevent from these attacks, it is essential to utilize various security mechanisms such as user authentication, key distribution, and user access control mechanisms. The most critical design parameter catering to security is authentication. Many social, tailored, or opportunistic assaults can compromise current authentication techniques such as the traditional knowledge factor. It's also quite pricey to make the switch from antiquated infrastructure to modern security measures. Expertise, possession, and inherence are three methods that can be used for user authentication. As its name implies the requirement for identity verification demands for some sort of information that a user should be familiar with it.

Common activities like entering login information fall within this category. This approach assumes the username is known to the public and the password is known only to the user. However, with the real experiences in the real world have taught us, passwords aren't always easy to keep safe, and the human mind isn't great at juggling a lot of different passwords for different services [9].

For ensuring security for both the users and the website, different types of authentication methods are available for use in Web Apps. Authentication is utilized not only on websites but also across a wide range of applications. It is an 'idea' to keep hackers away, so if they are not authorized to access, how could they hack the platform? When a user is authenticated, they may not have permission to access certain routes or perform tasks like entering the admin panel or deleting other users' posts. Both authorization and authentication collaborate to maintain the core security of the website; eliminating either of them would result in a sacrifice of the app's security. Authenticating the user holds no purpose if we do not grant them authorization for tasks and routes. Similarly, if authorization is implemented without authentication, users would find themselves unable to verify their identity for accessing the website [5].

The development of various identification, authorization, and authentication methods has been greatly influenced by the Internet. However, it has also made it easier for false identities and anonymous activities. In today's era, with approximately 46% of the world's population having Internet access, it is crucial to ensure secure user authentication. Therefore, impersonating a genuine user can lead to data theft and frauds. The risk of compromising authentication credentials increases due to password breaches, which can be attributed to increasingly sophisticated (and possibly targeted) phishing attacks or a large number of password database leaks. In the present day, the security of authentication holds a vital role for any server or website [6].

The current authentication methods include password-based authentication, biometric authentication, and hardware-based authentication. Password-based authentication stands as the most common authentication method; however, it faces challenges due to the prevalence of simple and easily guessable passwords, as well as the practice of using the same password across several services, which might also lead to dictionary or guessing attacks. Identifying the most secure authentication technique with high user acceptability poses a significant challenge because numerous threats can create loopholes in the authentication process [4].

The existing user authentication methods face challenges in protecting data from insiders due to the following loopholes: (i) Insiders can easily guess the user's password. (ii) The two-factor authentication approach, such as Google Authenticator (GA), which sends codes to users via Short Message Service (SMS), is not entirely secure. Attackers can potentially crack the SMS codes in the case of a security breach, risking the compromise of all user authentication codes. (iii) In the case of GA and other Third-Party Authentication Applications (TPAA), a single identity owns all authentication codes, making the system more vulnerable.

Over the years, different level authentication systems using encryption techniques have been presented however, the security provided by these methods are not up to the mark. In order to solve these issues, design and implementation of a server independent three level authentication system is presented. The remaining portion of the work is structured as follows: Section II provides a description of the literature survey. The section III describes the design and implementation of a server independent three level authentication system. The section IV demonstrates the result analysis. The section V ends with conclusion.

II. LITERATURE SURVEY

Qi Xie, Bin Hu, and Zixuan Ding et al. [11] describe An Anonymous Authentication Scheme Ensuring Security and Privacy with Three Factors for Wireless Sensor Networks in the Internet of Things. They present a new anonymous authentication scheme with three factors, using Elliptic Curve Cryptography (ECC). Using both formal and informal security analyses, this scheme can withstand different known attacks while maintaining computational complexity at a low level.

Abdelhafid Zitouni, Leila Megouache, and Mahieddine Djoudi et al. [12] describe ensuring data integrity and user authentication in a multi-cloud environment. This approach comprises three key steps. Firstly, it involves establishing a private virtual network to ensure the security of data during transit. Secondly, it utilizes data encryption as an authentication method to secure both the user's identity and their data. Lastly, the approach implements an algorithm to verify the integrity of data spread across the different clouds within the system. The model achieves both identity verification and the ability to facilitate communication between processes operating on various cloud providers. Additionally, a data integrity algorithm is showcased. The outcomes demonstrate that this model decreases the occurrence of unauthorized access by malicious individuals and reduces the time required for establishing a pathway through the virtual private network.

Teh Teck Guan, Siti Rahayu Selamat and Robiah Yusof et. al.,[13] describes Enhanced Authentication for Web-Based Security Through Keystroke Dynamics. A system has been developed, comprising two integral parts: enrollment and verification. Subsequently, a prototype has been created to facilitate the testing process, encompassing three key modules: Registration, Server/Client Link, and Authentication and Retraining. Based on the testing results, the keystroke dynamic authentication system demonstrated successful implementation in a client/server environment. Additionally, the system exhibited a low Equal Error Rate (EER), indicating its effectiveness in providing enhanced system authentication. Looking forward, future improvements to the system can focus on enhancing performance, security, and the user interface.

Nisha Soms, Sudarshan Pattabiraman, and Poovanan A et. al., [14] describes Password Protection using Honeywords. In this approach, several fake passwords are created for each user's account. Using this method, the hashed password database will contain both genuine and fake passwords. In the event that the password file is broken by an adversary, it becomes challenging for them to distinguish the set of genuine passwords. If an intruder attempts to use any of the honeywords in place of the genuine password, the Honeyword model issues an alert, warning of a potential password file attack. Therefore, it poses a significant risk for an adversary to be detected. This work introduces a decoy mechanism to protect data from malicious users and to trace the IP address of the identified user to take action against the felony.

Prof. Kirti Rajadnya, Vaishnavi Birhade, Prathamesh Pasalkar, Prashant Sargar et. al., [15] describes Password Protection for Online and Offline Data. In this system, fist level contains simple alphanumeric password combinations. In second level of authentication, the RGB (Red Green Blue) color code pattern is used and in third level graphical password is used i.e. face detection and recognition. The user will have to go through the all three levels for successful authentication. This 3 level password system will provide high security to the system.

Gaurav Deep, Anand Nayyar, Rajni Mohana, Eklas Hossain, and P. Sanjeevikumar et. al., [16] describes Authentication Protocol for Cloud Databases utilizing a Blockchain mechanism. The suggested mechanism's algorithm and theorem have been presented to demonstrate its correctness and applicability. The suggested mechanism has been tested against denial of service, offline guessing, impersonation, and no replay attacks using the Scyther formal system tool. The results from Scyther demonstrate that the described methodology is robust and secure.

Summer Devlin, Jessica Colnago, Maggie Oates, Lujo Bauer, Chelse Swoopes, Nicolas Christin, and Lorrie Cranor et. al., [18] describes a approach who Explores the Adoption of Two-Factor Authentication at a University. The authors observed the implementation of a Two-Factor Authentication (2FA) system at Carnegie Mellon University (CMU). The user opinions and behaviors are explored around adoption, surrounding a mandatory adoption deadline. The results indicate that: (a) Users who adopted 2FA considered it somewhat annoying but generally easy to use, and they believed it enhanced the security of their accounts. (b) Users' experience with CMU Duo often resulted in favorable perceptions, occasionally leading to the adoption of 2FA for other accounts; and (c) There were variations among users in terms of their willingness to adopt 2FA. This approach has concluded suggestions for large-scale 2FA deployments, focusing on implementation design, maximizing adoption, strategic messaging, and the use of adoption mandates.

Guoai Xu, Chenyu Wang and Jing Sun et. al., [19] describes an Enhanced User Authentication Scheme Utilizing the Elliptic Curve Cryptosystem with Three-Factor Authentication for Wireless Sensor Networks. An improved scheme is introduced that demonstrates resistance to various attacks while possessing numerous desirable attributes. Afterward, authors verified the security of this scheme through a BAN (Burrows–Abadi–Needham) heuristic and logical analysis. Moreover, when compared to other related schemes, this approach exhibits significant advantages.

Daniel Hausknecht, Steven Van Acker, Andrei Sabelfeld et. al., [20] describes Measuring Login Webpage Security. In this analysis, the security of login pages is evaluated against a login attacker model. This model encompasses various threats, including man-in-the-middle network attackers, both with and without the ability to sign certificates from a trusted certificate authority. It also considers the presence of a third-party resource attackerThrough the execution of actual attacks on 51,307 login pages within the Alexa top 100,000, it was ascertained that a significant 62.8%, or 32,221 of these login pages, could be relatively easily compromised by a man-in-the-middle attacker. Furthermore, achieving this doesn't necessitate special certificate-signing privileges.

He, H et. al., [21] describes Privacy Protection for Node Location and Data in Wireless Sensor Networks. A novel architectural framework is introduced, which monitors user-specific patterns to differentiate between legitimate users and illegitimate users. This system strengthens the user authentication. The proposed engine determines the authentication score by evaluating the similarity of features between previous and current user behaviors. The simulation results indicate that the suggested approach can significantly enhance the overall system performance. This method analyzes user-specific patterns in network access and file system activity to create models representing normal behavior. Such models will help in distinguishing between normal use and anomalous use.

Shuang Jia, Danyang Qin, Songxiang Yang, Qun Ding, and ErfuWang, et. al., [23] present a Key Management Scheme and Lightweight Authentication for Wireless Sensor Networks. This approach introduces an efficient and lightweight Authentication and Key Management Scheme (AKMS) to address the problem of malicious nodes within networking processes. It provides a high level of security at a low cost. Under the requirement of mobile sensor node authentication, AKMS will generate keys dynamically and utilize them for security protection. Even in situations where the keys are captured or compromised, attackers can neither utilize the previous keys to cheat nor manipulate the authenticated nodes. The simulation results suggest that the proposed scheme provides enhanced security with decreased energy consumption, especially in the case of wireless sensor networks that include mobile sensors.

Dr.A.Chandrasekhar, R. Joseph Manoj, et. al.,[24] describes An Authentication system for web services that utilizes the analysis of web server logs. This paper introduces a novel authentication method that verifies a user's identity through the analysis of web server log files containing information such as the user's username, IP address, URL (Uniform Resource Locator), password, status code, date and time of request, and utilizes the ingress packet filtering method to detect IP address spoofing. This approach additionally assesses the resulting data and the performance of the suggested work. The performance analysis concluded that the system's ability to restrict fraudulent users is superior to other existing authentication systems, including username and password, attribute-based authentication systems, and third-party authentication. As a result, the security of web services is improved, and the proposed model effectively encourages requesters to actively and honestly participate in access control.

Hoon-Jae Lee, Bruce Ndibanje, and Sang-Gon Lee et al. [25] present Security Analysis and Enhancements of Access Control and Authentication in the Internet of Things. This work provides improvements for various facets related to the security gaps identified in the previous protocol. Additionally, they conducted an analysis of the suggested improvements through performance and security analyses, considering computation and communication costs, and compared these to recent research in the IoT domain using specific metrics. In conclusion, the outcomes of both security and performance analyses demonstrate that the enhanced protocol fulfills the requirements for key security services in the IoT, including confidentiality, authenticity, and integrity. Furthermore, it demonstrates improved efficiency with reduced communication costs.

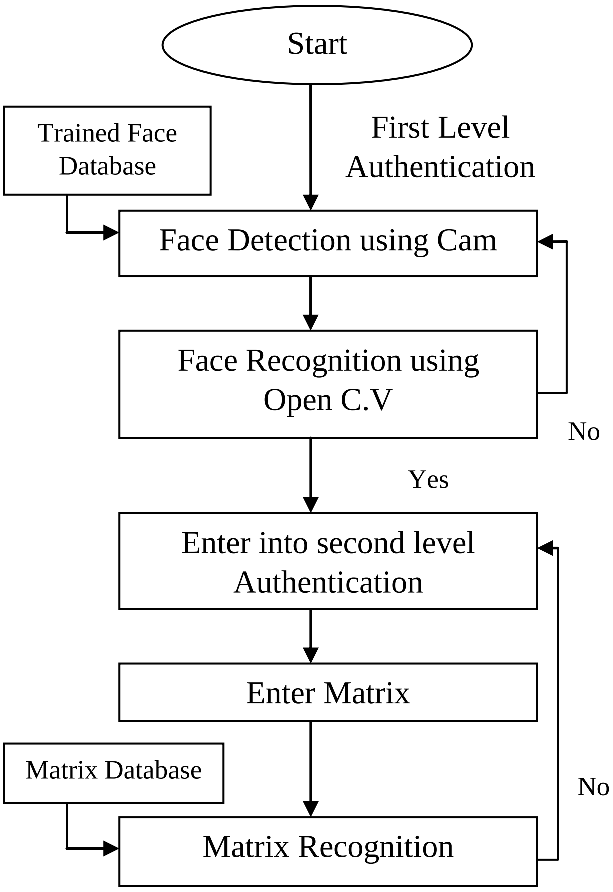
III. A SERVER INDEPENDENT THREE LEVEL AUTHENTICATION SYSTEM

Login pages play a critical role in the privacy and security of the private information of users on the web as they manage user login credentials. This work concentrates on analyzing secure systems for user authentication on a server. The importance of this focus becomes evident when considering that should an unauthorized user manage to pass the first barrier without the correct credentials, then the entire system could collapse, compromising all the user data (including physical addresses and email addresses) entered on the server, as well as passwords/websites (since people often use the same password for multiple accounts, such as their email and bank passwords, for convenience), potentially leading to significant security breaches.

As data becomes more confidential, there will be a simultaneous increase in security threats. Hence, there is a need for enhanced security in authentication, data protection, and system access. Multilevel protecting system will help us to protect the information. It will help us to overcome the vulnerabilities. By adding the extra levels in authentication, one can provide an enhanced security to the system. In this section, design and implementation of a server independent three level authentication system which will solve all the above mentioned problems. The figure 1 shows the workflow diagram of design and implementation of a server independent three level authentication system.

In this system, first the users have to register them self. In the registration process, the user need to give various information such as name, phone no., Email address. During the registration phase, his/her face is recognized and registered user faces are saved in the database. Whenever registered users are trying access the server then they need to go through following process. In this system, authentication is done three levels: i) User Face recognition; ii) Matrix Recognition and iii) Email and OTP recognition. The first level of authentication is user face recognition which is described as follows:

A dataset is trained with faces of various individuals which is crucial for building effective face recognition systems.



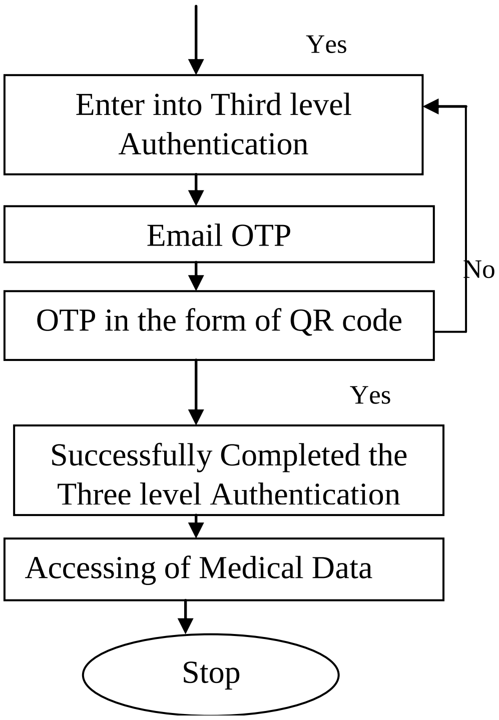

Yes
Enter into Third level Authentication
Email OTP
No
OTP in the form of QR code
Yes
Successfully Completed the Three level Authentication
Accessing of Medical Data
Stop

Figure 1: Workflow Diagram of a server independent three level authentication system

This permits the model to acquire a variety of facial features, resulting in an enhanced ability to identify various individuals. Face recognition is a technique used to identify or verify the face based on digital images captured by the camera. The fundamental concept of face recognition is based on the geometric features of a face. It is the practical and most intuitive method for facial recognition. Facial recognition is categorized as biometric software, which involves the mathematical mapping of an individual's facial features, storing the resulting data as a facial print.

OpenCV (Computer Vision) is a library consisting of programming functions primarily used for real-time computer vision applications. It serves as a cross-platform tool for creating such real-time computer vision applications. The main focus is on video capture, image processing, and analysis, which includes features such as face detection, object detection, and recognition. In this system, open CV is used to recognize the user faces. Facial recognition uses technology and biometrics through open CV to identify human faces. Facial recognition involves the mapping of facial features from a photograph or video, followed by a comparison of this information with a database of familiar faces to locate a match. This technology is valuable for confirming a person's identity. It performs a comparison between the input facial image and the user-associated facial image, which is a necessary step for authentication. If the user face is matched with dataset face then the user is allowed for second level authentication.

The second level authentication is Matrix recognition which is as follows: In the second level, matrix recognition is verified. A matrix database is a structured collection of organized data, or information, usually stored electronically within a computer system. The matrix database generates unique matrixes or patterns at a time which are displayed on the screen (for example 2x3 matrix), based on that matrix/pattern user enter the data. If the entered data is matched with the matrix database data, then second level authentication became successful and user is entered in to third level authentication.

At the third level of authentication, users are required to verify their email authentication. Email authentication stands out as one of the most commonly used authentication methods throughout the entire World Wide Web. It serves as the most widely used server system, enhancing not only the communication of data but also facilitating the secure transfer of data through email encryption. After the email authentication verification, OTP verification has to be done. A one-time password, commonly referred to as a one-time authorization code, dynamic password, or one-time PIN, represents a password that retains its validity for just a single session or transaction on a computer system or another digital device.

OTP generation algorithms commonly utilize pseudo-randomness to create a shared key or seed. They also utilize cryptographic hash functions. These functions are employed to generate a value that presents a significant challenge for an attacker in obtaining the original data used in the hash. It is essential because otherwise, predicting future OTPs by observing previous ones would be relatively simple. In today's day-to-day transactions over the network, OTP is becoming very popular. The primary benefit of OTP is that it eliminates the need for a password list. One-Time Passwords (OTPs) serve as an additional factor in multi-factor authentication/authorization applications. They are exclusively valid for a single authentication or authorization request. OTPs are delivered to the user via SMS, and the user's phone number must be registered with the service that issues OTPs for authentication or authorization. OTPs are widely used as an additional factor for authentication or authorization in web-based services.

Here in this system OTP will send after scanning the QR code. A QR code is a two-dimensional barcode format that, upon scanning with a mobile device, provides access to encrypted information related to the user's identity and OTP. If the entered OTP is matched then we will get medical data access. The person details like patient name, mail id, the disease that the patient have and doctor details, specialization of doctor and mail id. This approach provided three level authentications to medical server.

After successful three level authentications, the administration/ Hospital Management will know the basic information about the person and his past treatment through this server. Hence Hospital Management will access the server and medical data will be secured very effectively and accurate diagnosis is provided based on the details. In this way, there level authentication is provided. Hence, there is no chance for intruder to get the medical data. Therefore, this approach provides greater security and authentication to web servers as well as for user data.

IV. RESULT ANALYSIS

In this section, design and implementation of a server independent three level authentication system is implemented. The result analysis of server independent three level authentication system is evaluated here. The first step involves the registration phase, where users can register themselves into the system, but this step is only applicable to new users. The Figure 2 shows the registration form.

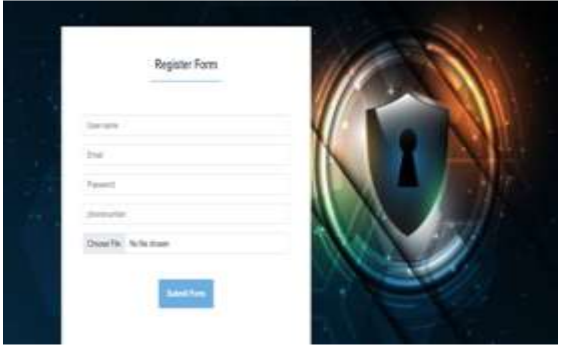


Figure 2: Registration Form

As the user is a new user then he/she needs to enter the details like UserName, Email address, Password, Phone Number, etc. During the registration phase, the user faces are recognized and faces are saved in the database. After the registration procedures, user face, details like name, phone number, email address are stored in the database. At fist level, user will have to submit Username. The system will authenticate the user and only authorised user can access the system. At the very first level, this system capture the user’s face and the system will try to match it with previously saved dimensions in order to authenticate the user. If it matches correctly then the user will move to next stage authentication. While entering in to a server, everyone needs to login to their accounts. If the user is registered one, then he/she needs to login to their accounts, if user is a new user then he/she needs to register. The figure 3 shows the first level authentication.

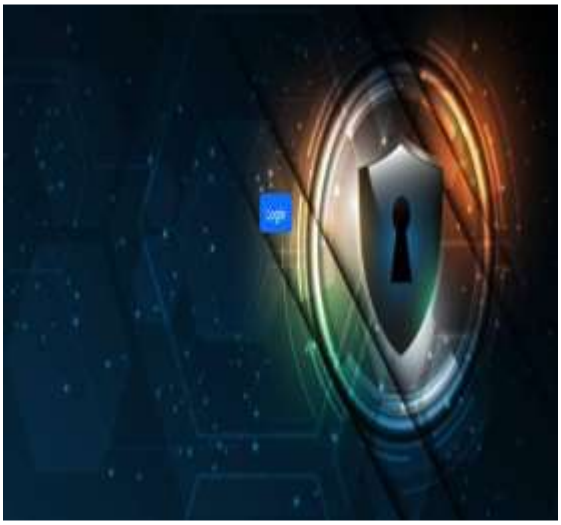


Figure 3: First Level Authentication

For the login, user has to submit the username and appropriate details to the system. During the login phase, users are enabled to authenticate themselves for the purpose of accessing the system's resources. If the user face is matched with the database then he/she is permitted to second level of authentication. The Figure 4 shows the second level authentication.

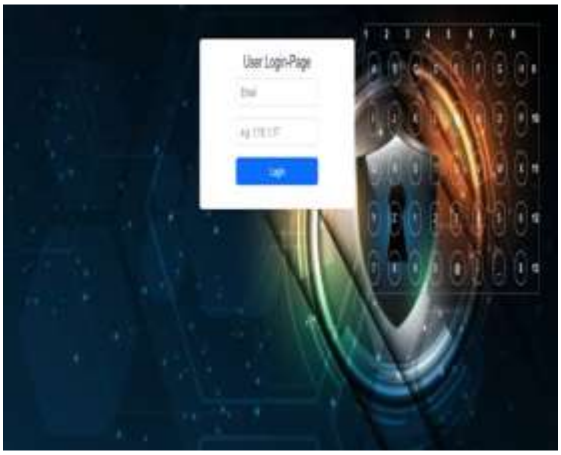


Figure 4: Second Level Authentication

At second level user should submit the correct matrix pattern code. The system will check whether the matrix pattern matches with the database pattern which is generated in a database. If the entered matrix pattern with the database pattern which was generated by matrix database, then the user will be moved to third level of authentication. The Figure 5 shows the Third level authentication.

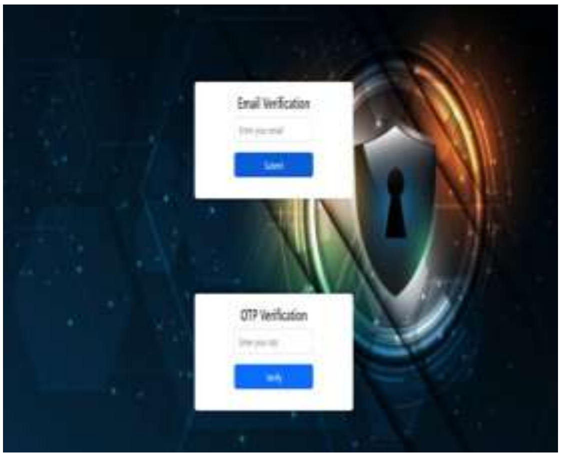


Figure 5: Third Level Authentication

At the last level of login phase, the system will need to provide the OTP which is sent through Email. If the entered email is corrected then the user needs to scan the QR (Quick Response) code which is sent to user mobile, after scanning the QR code user get a pin which is entered in the above screen to get access for medical server.

V. CONCLUSION

Login web pages serve as the initial access points to sensitive sections of web applications, including both user-specific access to website resources and public access to private ones. Therefore, it is crucial to prioritize the security of these entry points. To provide greater authentication to web servers, design and implementation of a server independent three level authentication system is presented in this work. In this system, the user authentications performed in three levels such as face recognition, matrix recognition, email and OTP verification. Firstly the users, need to register them self during the first visit. During the registration process, the user details are collected and saved in the database. In the first level, user face recognition is verified. If user face is matched then the user is moved to second level. At the second level matrix pattern need to be verified. The user moved to third level when second level is verified. In the third level, the user needs to verify the email and OTP for getting the access to the medical web server which contains details like patient basic information, his/her disease, previous doctor details and their specification. This approach authenticates user at three levels and these levels are unique. After successful authentication, the hospital management is able to access the server. As a result, this system provided greater authenticity and security to medical data.

VI. REFERENCES

[1] Ahmet Bucko, Kamer Vishi, Bujar Krasniqi and Blerim Rexha, "Enhancing JWT Authentication and Authorization in Web Applications Based on User Behavior History," Computers 2023, 12, 78, MDPI Journal, doi:10.3390/computers12040078,

[2] Sanam Ghorbani Lyastani, Michael Backes, Sven Bugiel, "A Systematic Study of the Consistency of Two-Factor Authentication User Journeys on Top-Ranked Websites (Extended Version)," Network and Distributed System Security (NDSS) Symposium 2023 27 February - 3 March 2023, San Diego, CA, USA ISBN 1-891562-83-5 https://dx.doi.org/10.14722/ndss.2023.23362

[3] Akanksha and A. Chaturvedi, "Comparison of Different Authentication Techniques and Steps to Implement Robust JWT Authentication," *2022 7th International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, India, 2022, pp. 772-779, doi: 10.1109/ICCES54183.2022.9835796.

[4] Sandeep kaur, Gaganpreet kaur, and Mohammad Shabaz, "A Secure Two-Factor Authentication Framework in Cloud Computing," Hindawi Security and Communication Networks, Volume 2022, Article ID 7540891, 9 pages, doi:10.1155/2022/7540891

[5] Piyush Pant, Anand Singh Rajawat, S.B. Goyal, Pradeep Bedi, Chaman Verma, MariaSimona Raboaca, Florentina Magda Enescu, "Authentication and Authorization in Modern Web Apps for Data Security Using Nodejs and Role of Dark Web," Procedia Computer Science, Volume 215, 2022, Pages 781-790,doi: 10.1016/j.procs.2022.12.080

[6] Adarsh Thapa, Chirag Singh Dhapola, Hemraj Saini, "Security Analysis of User Authentication and Methods," 2022 Association for Computing Machinery, ACM ISBN 978-1-4503-9675-2/22/08,https://doi.org/10.1145/3549206.3549304

[7] R. F. Olanrewaju, B. U. I. Khan, M. A. Morshidi, F. Anwar and M. L. B. M. Kiah, "A Frictionless and Secure User Authentication in Web-Based Premium Applications," in *IEEE Access*, vol. 9, pp. 129240-129255, 2021, doi: 10.1109/ACCESS.2021.3110310.

[8] Merja Laamanen, Tarja Ladonlahti, Sanna Uotinen, Alexandra Okada, David Bañeres and Serpil Koçdar, "Acceptability of the e‑authentication in higher education studies: views of students with special educational needs and disabilities," Int J Educ Technol High Educ (2021) 18:4, https://doi.org/10.1186/s41239-020-00236-9

[9] Balkis Bettoumi and Ridha Bouallegue, "LC-DEX: Lightweight and Efficient Compressed Authentication Based Elliptic Curve Cryptography in Multi-Hop 6LoWPAN Wireless Sensor Networks in HIP-Based Internet of Things," Sensors 2021, 21, 7348. https://doi.org/10.3390/s21217348,

[10] Victor R. Kebande, Feras M. Awaysheh, Richard A. Ikuesan, Sadi A. Alawadi and Mohammad Dahman Alshehri, "A Blockchain-Based Multi-Factor Authentication Model for a Cloud-Enabled Internet of Vehicles," Sensors 2021, 21, 6018, MDPI Journal, https://doi.org/10.3390/s21186018

[11] Qi Xie , Zixuan Ding , and Bin Hu, “A Secure and Privacy-Preserving Three-Factor Anonymous Authentication Scheme for Wireless Sensor Networks in Internet of Things,” Hindawi Security and Communication Networks, Volume 2021, Article ID 4799223, 12 pages, https://doi.org/10.1155/2021/4799223

[12] Leila Megouache, Abdelhafid Zitouni and Mahieddine Djoudi, “Ensuring user authentication and data integrity in multi‑ cloud environment,” Hum. Cent. Comput. Inf. Sci. (2020) 10:15, doi:10.1186/s13673-020-00224-y

[13] Siti Rahayu Selamat, Teh Teck Guan and Robiah Yusof, “Enhanced Authentication for Web-Based Security Using Keystroke Dynamics,” International Journal of Network Security & Its Applications (IJNSA) Vol. 12, No.4, July 2020, DOI: 10.5121/ijnsa.2020.12401

[14] Sudarshan Pattabiraman, Nisha Soms and Poovanan A, “Password Protection using Honeywords,” Advances in Computing, Communication, Automation and Biomedical Technology, 2020, DOI: 10.46532/978-81-950008-1-4_001

[15] Prof. Kirti Rajadnya, Prathamesh Pasalkar, Vaishnavi Birhade, Prashant Sargar, “Password Protection for Online and Offline Data,” International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 07 Issue: 05, May 2020,

[16] Gaurav Deep, Rajni Mohana, Anand Nayyar, P. Sanjeevikumar and Eklas Hossain, “Authentication Protocol for Cloud Databases Using Blockchain Mechanism,” Sensors 2019, 19, 4444; MDPI Journal, doi:10.3390/s19204444

[17] Run-Fa Liao, Hong Wen, Jinsong Wu, Fei Pan, Aidong Xu, Yixin Jiang, Feiyi Xie and Minggui Cao, “Deep-Learning-Based Physical Layer Authentication for Industrial Wireless Sensor Networks,” Sensors 2019, 19, 2440, MDPI Journal, doi:10.3390/s19112440

[18] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, Nicolas Christin, “It’s not actually that horrible”: Exploring Adoption of Two-Factor Authentication at a University,” CHI 2018, April 21–26, 2018, Montréal, QC, Canada, ACM ISBN 978-1-4503-5620-6/18/04, DOI: 10:1145/3173574:3174030

[19] Chenyu Wang, Guoai Xu and Jing Sun, “An Enhanced Three-Factor User Authentication Scheme Using Elliptic Curve Cryptosystem for Wireless Sensor Networks,” Sensors 2017, 17, 2946; MDPI Journal, doi:10.3390/s17122946

[20] Steven Van Acker, Daniel Hausknecht, Andrei Sabelfeld, “Measuring Login Webpage Security,” SAC 2017,April 03-07, 2017, SAC '17: Proceedings of the Symposium on Applied ComputingApril 2017Pages 1753–1760 2017 ACM, 978-1-4503-4486-9/17/04, http://dx.doi.org/10.1145/3019612.3019798

[21] He, H, “Privacy Protection of Node Location and Data in Wireless Sensor Networks,” *International Journal of Online and Biomedical Engineering (iJOE)*, Volume 12, Issue 11, 2016, pp. 34–39, doi:10.3991/ijoe.v12i11.6235

[22] Mrs. Ruma Rahul Kapre, “Authentication Techniques Help To Improve Security in the Era of Network System: A Study,” IOSR Journal of Computer Engineering (IOSR-JCE),2016, e-ISSN: 2278-0661,p-ISSN: 2278-8727 PP 01-06

[23] Danyang Qin, Shuang Jia, Songxiang Yang, ErfuWang, and Qun Ding, “A Lightweight Authentication and Key Management Scheme for Wireless Sensor Networks,” Hindawi Publishing Corporation, Journal of Sensors, Volume 2016, Article ID 1547963, 9 pages http://dx.doi.org/10.1155/2016/1547963

[24] R. Joseph Manoj, Dr.A.Chandrasekhar, “An Authentication system of Web Services Based on Web Server Log Analysis,” International Journal of Engineering and Technology (IJET), Vol 5 No 6 Dec 2013-Jan 2014, ISSN : 0975-4024,

[25] Bruce Ndibanje, Hoon-Jae Lee and Sang-Gon Lee, “Security Analysis and Improvements of Authentication and Access Control in the Internet of Things,” *Sensors* 2014, *14*, 14786-14805; doi:10.3390/s140814786