JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Enhanced Multi-factor authentication System using Biometric Sensing in the Medical Sector

Abdulrahman Muhammadi[1], Vijayakumar Adaickalam[2]
[1]*Final Year PG Student, School of Computer Science and Information Technology, Jain Deemed-to-be University, Bengaluru*
[2]*Professor, School of Computer Science and Information Technology, Jain Deemed-to-be University, Bengaluru*
Email: abdulrahmanmuhammadi007@gmail.com[1], vijay.pattukkottai@gmail.com[2]

Abstract: Safe and secure login to a website and web application is very difficult to guarantee when it's taking longer to log in to the account. At the beginning of 2020, the world was hit by a pandemic. This led the world to adapt and transition from offline to online. With this change occurred plenty of data breaches and disclosures were seen. A lot of vulnerabilities were discovered and filled. Activities that could have been done in person transitioned to online such as education, entertainment, medical, and many more. The most vulnerable domain was and is the medical sector. A new and improved Authentication system has been proposed to safeguard this sector, which has multiple security factors and authenticates the authorized user's identity on several layers. Increasing the security and fortifying the system from the start. The proposed system consists of five factors, namely: Knowledge, possession, time, location, and inherence factors. Each of these factors will be used to verify the identity of the user and authorize him/her to use the system.

Keywords: Multi-factor authentication, Biometric Factors, Time Factor, Geolocation Factor, Possession Factor.

1. Introduction

MFA started from SFA then it moved on to 2FA and now most organizations rely on MFA. Multi-factor authentication has become very important for authenticating the identity of the user and securing information. Multi-factor authentication (MFA) is a security mechanism that uses several security factors (security measures) when determining the identity of the user. Logical and Physical security in the medical facility is very much important. Physical security refers to securing the facilities and preventing intruders or malevolent attacks from physically harming the company, its personnel, or its property. On the other hand, securing the data, information, and systems of the medical institute is also very essential which comes under Logical security. All information on patients, system users, healthcare staff, and doctors should be kept secure and handled safely and securely. A Simple Multi-factor authentication consists of different Authentication factors, namely: Knowledge Factor, Possession Factor, and Inherence Factor.
The above-mentioned factors are common in every multi-factor authentication system; however, the question arises of how these factors can be integrated to stop the breaches and data loss or corruption when an attack occurs in the medical sector. The proposed architecture focuses on the combination of Authentication factors of the MFA, by implementing various security mechanisms and achieving more security for the system which are being utilized in the medical sector. The authorized user while being verified by the system won't be authorized every time by the same combination of security factors. For every instance of the verification, the combination of the factors may change or remain the same. Predominantly, the project works on the combination of different factors the legacy factors as well as the time and location factors too. Every text box for entering the required information has been verified, validated, and encrypted. The password, which is the knowledge factor, is encrypted and then stored in the database. The possession factor, which is used in this project, is a One-time Password that is randomly generated by the system and sent to your registered email address at the time of creation. The OTP can be extended up to 18 digits the default being 6 digits. In the proposed system new factors of MFA have also been used namely: Location and Time-based factors. Location factor verifies the identity of the user based on his/her IP address and verifies the network with which they have connected to the system. If the user is connected via a different network, the system will flag the user and restrict his or her access to the system. Session-based time, from the time the user puts in his username and password, till the time the user receives the OTP, the session will be monitored based on the time and if the user takes more time in submitting the OTP, the session will be timed out or the session is kept ideal for a long period these

are the red flags for the system. In the proposed system the user has the option of choosing between knowledge and the inherence factor for the login. Which gives the user an extra layer of security and choice.

2. Related Work

J Liou et al. [1] have proposed a secure and safe RFAA (RFID Factor Authentication Application) model for multi-factor authentication as a SofToken that acts as a security factor. When the proposed model was compared with other security factors the RFAA scored higher based on its security architecture. But again, the issue remains with the human factor of the authentication. S. Chaudhari et al. [2] have proposed a system that has been designed, implemented, and integrated for a multi-layered, multi-factor authentication setup for securing the webmail application, using various freeware open-source tools. The implementation ensures the fulfillment of varying authentication requirements for Intranet, Internet, and Extranet webmail users. Hussain et al. [3] have proposed a comparison between the use of SSO and MFA when it comes to AAAA (Authentication, Authorization, Accountability, Availability) in a cloud environment. According to the authors, MFA performs better than SSO to guarantee AAAA. Nwabueze et al. [4] proposed an Enhanced MFA for mobile phones' 4G wireless network. Their proposed system consists of the following factors namely, Knowledge, possession, and the Inherence factor. The proposed system is cost-effective, flexible, and convenient even for remote users. Sanchari Das et al. [5] tried to address the literature gap which exists in the implementation and design of a multi-factor authentication system. The author proposed that most of the work regarding multi-factor authentication by different researchers is very new. Kim and Hong [6] have improved the user authentication level systems model into 5 stages. They proposed the public key infrastructure for the first stage and biometric authentication for the fifth stage. They have divided their research into 3 major stages. First is the evaluation of the improved UALS model, second is that the model can be used for high-risk transactions and third is the risk assessment based on the MFA. Adil Hussain et al. [7] have proposed that the data of the medical sectors are very much susceptible because they are breached by outsiders as well as insiders. This paper gives us a grim reality for our data and how it's easy for an attacker to hack our data and infiltrate our privacy. Haqi Khalid et al. [8] have proposed that to stop unauthorized access to the fog servers a new secure and lightweight multi-factor authentication scheme for cross-platform IoT systems (SELAMAT) has to be implemented. The scheme has been tested and compared extensively using the AVISPA tool, which is a reliable tool for security testing. W. Li et al. [9] have proposed a new way of verification for the users who want to access the system. They have designed a new threshold MFA key exchange protocol on top of their design for the MFA system. Guma Ali et al. [10] have proposed a better security mechanism for mobile money transfer and transactions, with multiple security mechanisms and factors in a place like, QR, biometric, OTP, and all the factors are being encrypted using the secure hashing algorithm of 256bits. Fatima K et al [11] proposed behavioral biometric access in the medical sector. With the use of different biometric factors, unauthorized access to the data and system in the medical sector can be drastically mitigated. Tahir et al. [12] proposed in their paper the merging of 5G technology with different aspects of the healthcare sector. The role of this new technology will be prominent in the sector such as security, communication, and network, and the most important is the merging of 5G and IoT for smart healthcare. The opportunities it will have in the research and technology of new systems in the healthcare sector are eminent. OneLogin [13] in one of their articles has mentioned that MFA can't guarantee foolproof security or stop malicious actors. However, it can safeguard high-value systems and accounts and limit the usefulness of stolen credentials. ISA Cybersecurity [14] mentions that the medical sector is a prime target for malicious attacks in terms of cyber-attacks because of the huge amounts of data. They have defined a few ways to create a security culture among the employees so that they can at least be more aware. Should have a strong classification of data. Strong access control should be in place. And the data should be backed up regularly based on the importance the data. Steven Bowcut [15] in his article writes about the security in healthcare that once when the criminals get their hands on the medical data of the patients, they sell them on the dark web for different types of scams and frauds. The ransomware attack has become so common in the medical sector because the medical sector is a very lucrative and important sector of our society. The medical sector should be safeguarded against different types of attacks because, in case of any type of disruption of problem, it's a matter of life and death.

3. Proposed System

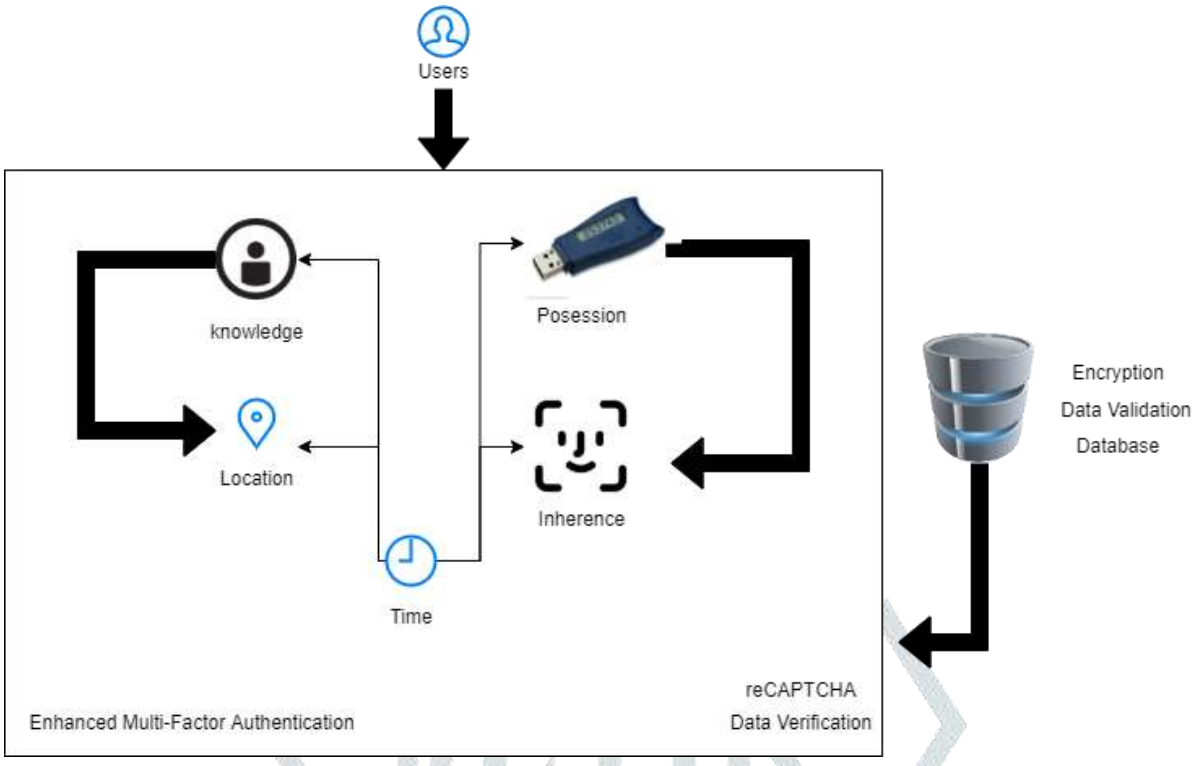

Fig 1: Enhanced Multi-factor Authentication with different security factors

3.1 Technical Background:

PHP and JS are used throughout the implementation, along with the bootstrap and MySQL for the backend. The project can be implemented with any other web application or website. For the basic design of the system, we have used Bootstrap and CSS. Implementing various Libraries and frameworks namely: PHP mailer and reCAPTCHA. XAMPP is used for the implementation and using the localhost as a webserver, where Apache tomcat and MySQL are running for the implementation and sublime is used as a code editor. PHP mailer is used to implement the mechanism of sending OTP automatically from one email given in the code to the registered emails, which are in the database. The code can be implemented and run in any system, which has XAMPP installed in it and it can be connected with any other web application or website. The analysis and the testing of the systems are done in a windows environment and no issues and errors have been detected. The password is encrypted using "md5 128 bit", and stored in the database. Form validation is implemented in the multi-factor authentication system. OTP is a randomized number of 6 or more digits that can be incremented and decremented based on the size. The IP addresses of the systems are also being stored in the database which verifies the location of the user from where he/she is accessing the system. The IP address is stored to verify the geo-location factor of multi-factor authentication. The backend of the system is encrypted. For the backend, there are 2 separate databases for the login details. One is for the registration of the users and users trying to log in using username and password and the other one is for storing the face data for the face-recognition login.

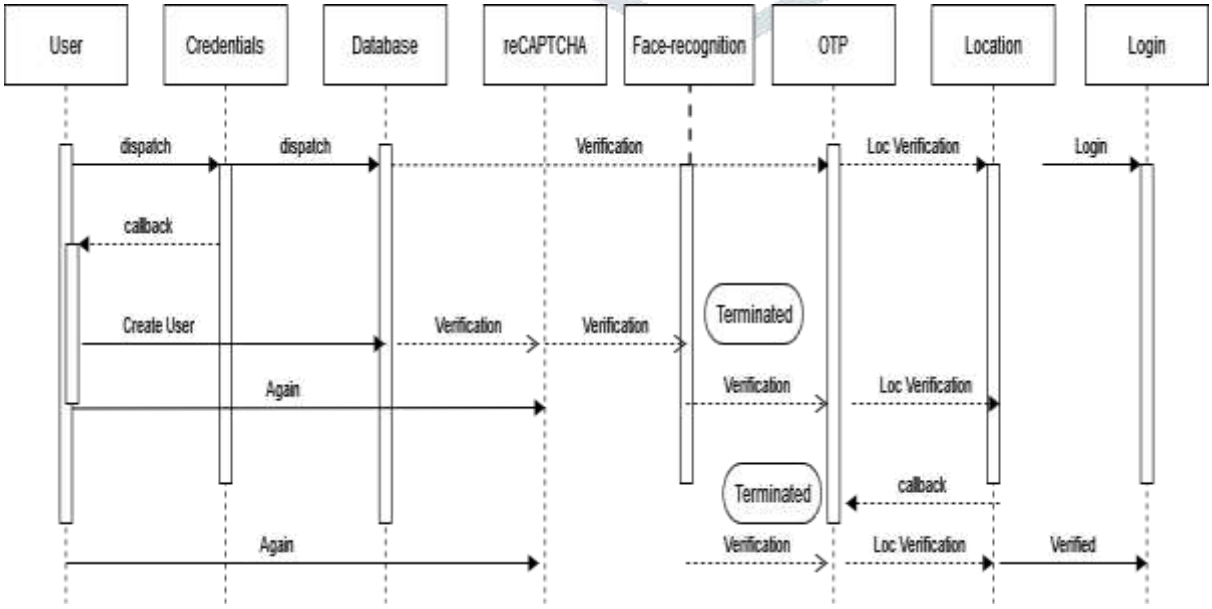

Fig 2: Sequence diagram for the enhanced multi-factor authentication

The sequence Diagram explains the sequence and how the complete process of Enhanced Multi-factor authentication takes place from the user to the login.

It is displayed in the below figure how all the steps are done in sequential order once after the other. The below figure explains clearly what all takes place in the system and all the verifications and the reCAPTCHA verification, OTP Verifications, Location Verification, Face-Recognition, and last but not least Password and Username. Retrieval of data from the database and storage of data to the database. The system works perfectly. If the website or web application is built using the same technology, it's very easy to merge this code with that and boost the security and access control to that system.

3.2 Security factors:

Knowledge Factor: The username and password are very important in any system, the proposed system also has a knowledge factor which is the very first step in verifying the identity of the user. The password is stored using md5 128-bit encryption in the database. The verification of the password is done twice. First while registering it should have all the necessary combinations of letters, numbers, special characters, and capital and small letters, this is known as password validation, and the second time when the user location is being verified, which will be explained further in the document.

Possession Factor: The possession factor is a very important factor of the MFA system, where it verifies the user's identity twice using an OTP generator, an app, a cellphone, or the registered user's email. OTP stands for one-time password and it's a basic combination of numbers, alphabets, or just numbers. The OTP generator of the proposed system can generate 6 random digits but I can program it to generate more than 6.
The OTP generator with the proposed system can work with any email service, for the implementation of the OTP generator library from PHP, the PHP mailer has been used to send automated emails to the registered email addresses during the sign-in process. As long as the registered email is correct there won't be any issues faced while receiving the OTP. In case you have typed a wrong OTP or if you haven't received the OTP, you can press the resend button and the system will resend the OTP to the registered email address.

Inherence Factor: Inherence factors are metrics intrinsically owned by the authorized individuals. These often take the form of biometrics – such as fingerprint readers, retina scanners, face recognition, or voice recognition. These inherence characteristics are nearly 100 percent unique to the authorized user, ensuring that unauthorized users cannot complete the authentication procedure.

In today's technology, biometric authentication is becoming more robust and ubiquitous. Biometric authentication technology is currently found in everyday cellphones and laptops, and its application in multi-factor authentication will only become more advanced and widespread. Online bank transactions are an example of a regularly utilized multi-factor sign-in system. To strengthen the security of the identity identification process, many banks require the entry of customer numbers, passwords, and PINs, as well as the usage of a card reader.

Time Factor: The time factor starts from the user running the proposed system till the login. In case of a delay or the system being idle for a long period which is not normal, the session will automatically time out and the verification should start from the beginning.

Location factor: Location-based MFA usually looks at a user's IP address and, if possible, their geo-location. This information can be used to simply prohibit a user's access if their location information does not match what is defined on a whitelist, or it can be used as an extra form of authentication with other factors like a password or an OTP to validate that user's identity. The location factor is another very important factor in MFA, which verifies whether the person is accessing the system from an authorized location that is stored at the time of registration, this factor minimizes the threat of internal attacks from disgruntled employees or insider threats. In case someone has been the victim of social engineering attack and has shared their password and username with some hacker. Still, the hacker should be inside the building or should be connected to the same network which is already stored in the database.

Additional features: All the data of the users have been encrypted and stored in the database. Safeguard against Bot attacks, a reCAPTCHA security mechanism has been implemented. Each piece of information is validated and verified before storage in the database.

4. Results and Discussion

The system validates and checks each piece of identity from OTP to the saved face and verifies it with the already saved data, to ensure the maximum amount of security and mitigate unauthorized access and data breaches. For face recognition, the Face API is used from Microsoft Azure. The face is recognized and stored during the registration. OTP is sent to the registered email for verification. The system gives you the option of signing in using the username and password or using face recognition. For each of these factors, first, the user should be registered with the system. The possession factor of the system sends an OTP to the registered Email ID. The Geo-location facto verifies the IP address of the user upon inserting the username and password or the Face. The Time factor is the overall time from the start of the system till the user gets access to the homepage.

Apart from the security factors, the proposed system also has some other security features such as reCAPTCHA, Encryption of the saved data in the database, and data validation and verification while creating the account. The system performs well with the controls and unauthorized access is mitigated. All the features of the proposed system can be used once the user registers himself or herself in the system. If the users are already registered in the database, you can insert the username and password or use your face as an inherence factor to login into the system, verify the reCAPTCHA and access the system. The Database for the proposed system is defined and stored in form of MySQL. The database has data validation in place for each cell. The data which is been asked by the users is used for retrieving the forgotten password which is a part of future enhancement. Another security mechanism of reCAPTCHA which is a free Google service to mitigate Bot attacks is also been used in the system. Once the details are filled in the registration form the user needs to complete the reCAPTCHA and confirm his/her identity as a human. Once that is done you can save the details in the database. The proposed system also has a possession factor that sends an OTP to the registered email address. After verification, only the system will allow the user to enter the homepage. Following are a few of the screenshots of the system.

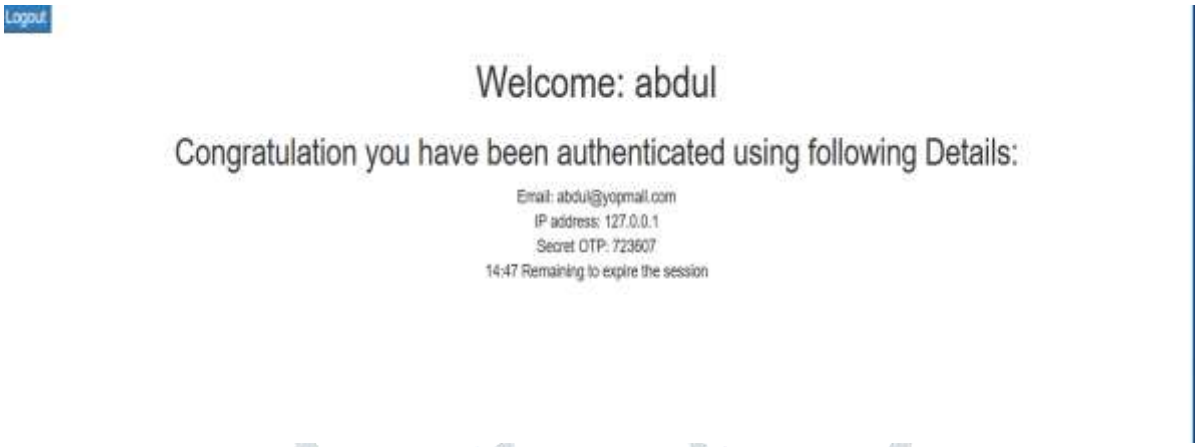

Fig 1: Final Outcome of the System

The system verifies the authorized user based on the certain criterion which is mentioned in the outcome figure 1 of the paper.

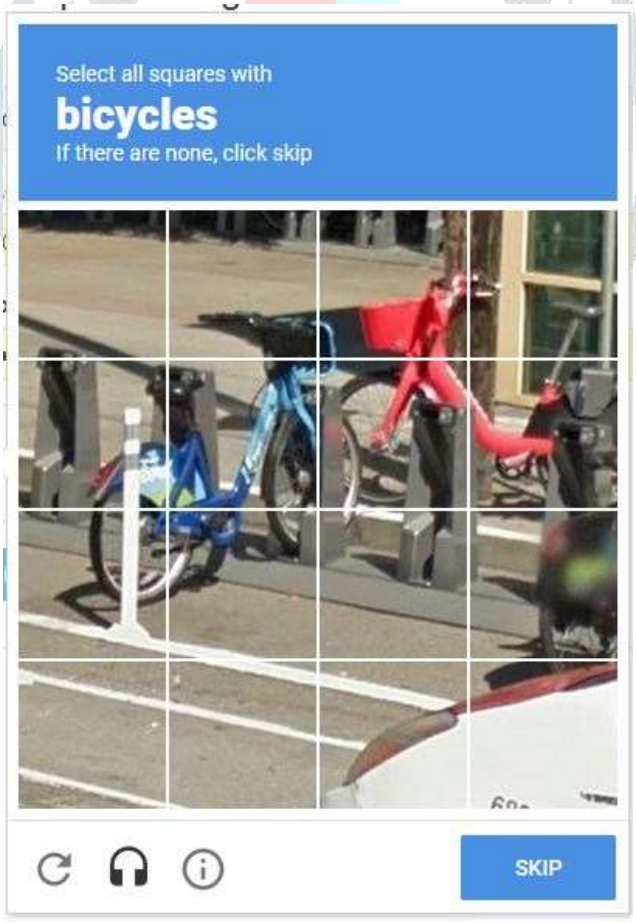

Fig 2: reCAPTCHA for Bot Attacks

reCAPTCHA is a google based security mechanism, that uses AI to differentiate between a human and a bot. reCAPTCHA is a free service from Google that helps protect websites from spam and abuse.

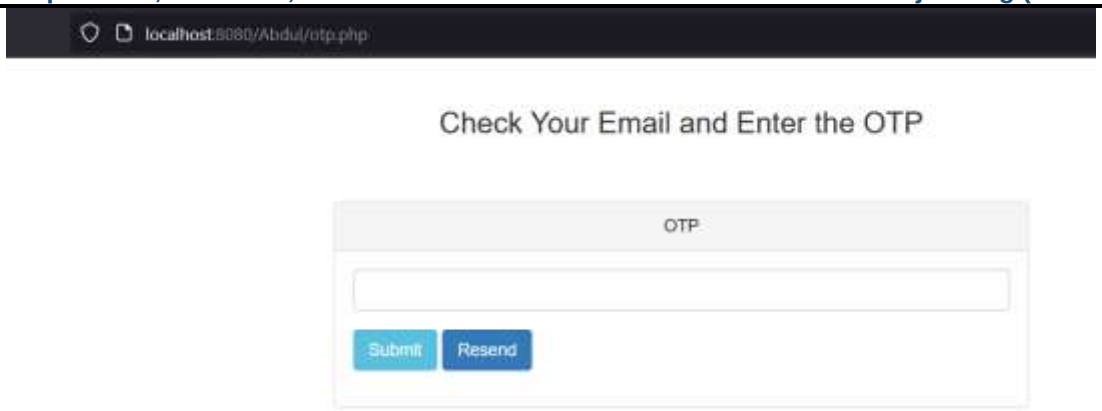

Fig 3: Possession Factor of the system

One-time password (OTP) systems provide a mechanism for logging on to a network or service using a unique password that can only be used once. Using the OTP you can gain access to the system, or the MFA will allow you to enter.

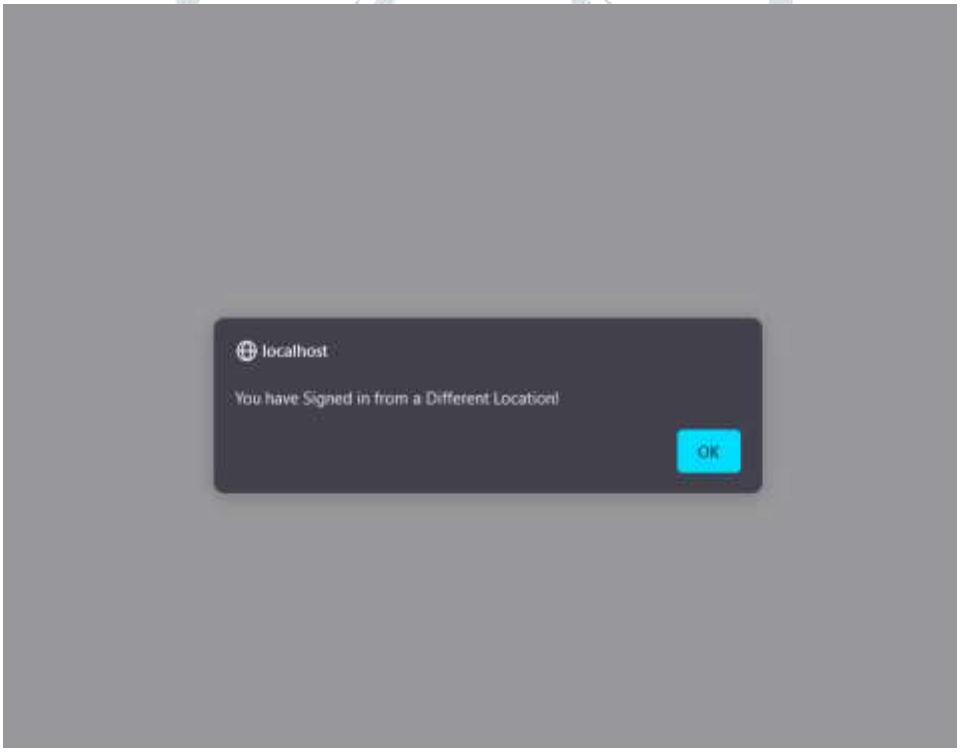

Fig 4: Geo-location Factor

If the IP address doesn't match what is stored in the database, the process will terminate. At the time of the registration, the IP address is also stored in the database. Before inserting the OTP, which is sent to the registered email address, first, the IP address is verified.

5. Conclusion & Future Enhancement

The proposed system provides a secure and safe gateway to any web application system; it can be easily implemented and merged with any code of the same language. The proposed system provides multiple layers of security. Each of these is used to verify the identity of the user and to mitigate unauthorized access and data breaches in the medical sector. A few key features and functions the multi-factor authentication system can carry out are Validation of the data. Factors for MFA are namely; Knowledge Factor, Possession Factor, Time Factor, Location Factor, Inherence Factor. Apart from the factors, a few more security mechanisms are multi-Layer security mechanisms, Encrypted passwords, Custom OTP Generation, reCAPTCHA, and the proposed system can be easily merged with any code of the same language. Implementing the proposed system with AI, Password recovery, adaptive MFA, and Push authentication are a few of the features which need to be added to the proposed system to make it more accessible to a larger audience. Inclusion of Pin code is also another means of knowledge factor which would work best for the proposed system. The AI aspect of the proposed system will generate the security factors at random for authorizing the user. In this way, the malicious actor can't predict which factor will pop up for the authorization.

6. References

[1] J. Liou, G. Egan, J. K. Patel, and S. Bhashyam, "A Sophisticated RFID Application on Multi-Factor Authentication," 2011 Eighth International Conference on Information Technology: New Generations, 2011, pp. 180-185;

[2] S. Chaudhari, S. S. Tomar, and A. Rawat, "Design, implementation, and analysis of multi-layer, Multi-Factor Authentication (MFA) setup for webmail access in multi trust networks," 2011 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), 2011, pp. 27-32;

[3] Hussain, M.I.; He, J.; Zhu, N.; Sabah, F.; Zardari, Z.A.; Hussain, S.; Razque, F. AAAA: SSO and MFA Implementation in Multi-Cloud to Mitigate Rising Threats and Concerns Related to User Metadata. Appl. Sci. 2021, 11, 3012;

[4] Nwabueze, E.E., Obioha, I. and Onuoha, O. (2017) Enhancing Multi-Factor Authentication in Modern Computing. Communications and Network, 9, 172-178;

[5] Das, Sanchari & Wang, Bingxing & Tingle, Zachary & Camp, L... Evaluating User Perception of Multi-Factor Authentication: A Systematic Review, 2019;

[6] Kim, Jae-Jung & Hong, Seng-Phil. (2011). A Method of Risk Assessment for Multi-Factor Authentication. JIPS. 7. 187-198;

[7] Adil Hussain Seh, Mohammad Zarour, Mamdouh Alenezi, Amal Krishna Sarkar, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan, "Healthcare Data Breaches: Insights and Implications", Healthcare Basel MDPI, Vol. 8, no 2, 2020;

[8] Khalid, Haqi, Shaiful J. Hashim, Sharifah M.S. Ahmad, Fazirulhisyam Hashim, and Muhammad A. Chaudhary. 2021. "SELAMAT: A New Secure and Lightweight Multi-Factor Authentication Scheme for Cross-Platform Industrial IoT Systems" *Sensors* 21, no. 4: 1428;

[9] W. Li, H. Cheng, P. Wang, and K. Liang, "Practical Threshold Multi-Factor Authentication," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 3573-3588, 2021;

[10] Ali G, Dida MA, Elikana Sam A. A Secure and Efficient Multi-Factor Authentication Algorithm for Mobile Money Applications. *Future Internet*. 2021; 13(12):299;

[11] Fatima, K., Nawaz, S., & Mehrban, S. (2019). *Biometric Authentication in Health Care Sector: A Survey. International Conference on Innovative Computing (ICIC).* pp 1 – 10, 2019;

[12] Tahir, Mohammad & Yau, Kok-Lim. 5G-Based Smart Healthcare Network: Architecture, Taxonomy, Challenges and Future Research Directions. IEEE Access. PP. 1-1. 2019;

[13] How MFA helps prevent common Cyberattacks https://www.onelogin.com/learn/mfa-types-of-cyber-attacks;

[14] Cybersecurity in Pharmaceutical Industry, https://isacybersecurity.com/cybersecurity-in-the-pharmaceutical-industry/ August 2020;

[15] Steven Bowcut, Cybersecurity in Healthcare, Cybersecurity Guide, https://cybersecurityguide.org/industries/healthcare/, February 2019;