iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52098

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Authentication System for Enterprise Security

Sourabh Suman[1], Abhinav Raj[2], Ashish Kumar[3], Prof. N.G Bhoskar[4]
[1, 2, 3]*Student, Dept. of Electronics and Telecommunication Engineering, Sinhgad College of Engineering, Maharashtra, India*
[4]*Assistant Professor, Dept. of Electronics and Telecommunication Engineering, Sinhgad College of Engineering, Maharashtra, India*

Abstract: ***Authentication plays a central role in boosting an organization's security posture. It helps enable an organization to keep its systems secure by permitting only authenticated users (or processes) to access the protected resources, such as computer systems, networks, databases, websites, and other network-based applications or services. Passwords are the more traditional form of authentication, but they constitute a weak form of protection; users are prone to bad password practices, such as reusing passwords, using predictable passwords, or even sharing passwords with others. To combat this issue, more companies are leveraging artificial intelligence (AI) and machine learning (ML) technologies, such as deep learning-based techniques, to develop better and more secure authentication approaches. AI/ML algorithms have been shown to bolster cybersecurity by protecting devices against cyber-attacks and preventing fraudulent activities. In this blog post, we introduce an AI solution based on deep learning and computer vision to perform face recognition-based biometrical authentication. So, what exactly does face recognition do? Face recognition is a broad problem of identifying or verifying a person in digital images or video frames through facial biometric patterns and data. The technology collects a set of unique biometric data of each person associated with their face and facial expression to authenticate a person. Face recognition technology is mostly used for two types of tasks:***
Face Verification: given a face image, match it with known images in a secure database, and give a yes/no decision.

I. INTRODUCTION

We provide a self-guaranteed secure program and its successful methods to overcome the risks of illegal attacks. This method ensures the security of a program by giving method-level security that bolsters the further implemented security measures. One of the most common computer authentications is for a user to submit a username and text password but the vulnerabilities of this method are plenty One of the main problems that could arise is the difficulty of remembering passwords. Studies have shown that user usually tends to pick short passwords so that the passwords are easy to remember. These passwords can also be guessed. To protect any system, authentication must be provided so that only authorized persons can have the right to use or handle that system and data related to that system securely. In order for the authentication system to be practical, three-level authentications are designed to provide additional security. There are many schemes that had been proposed but still have their weaknesses. For our information, the three-level authentication is the combination of three existing scheme which is, pattern lock and one-time password (OTP) to form better protection One of the approaches normally in use is the common authentication procedure in which a user needs only a user name and password, in other to make use of an authentication and authorization system in which every client has the right to access the data and applications which are only appropriate to his or her job.

A. Problem Statement

Authentication is an activity to authenticate the person's credential that wishes to perform the activity. In the process of authentication, the password entered by the user will be transmitted along the traffic to the authentication server in order to allow the server to grant access to the authorized user. When the password is transmitted, the attackers will try to sniff into the network to obtain data that include the user's password. Currently, there is a rainbow table which able to trace the password with the hash algorithm to obtain the user's password. Once the password is succeeded to be decrypted, the attackers can use the user credential to do something illegal such as fraud others which will cause the user to lose in credit. According to Pagliery(2014), there is 47% of the American adults accounts been hacked in that year. Their personal information is exposed by the hackers. Due to the problem exists, there are more people no longer trust that password will be able to protect their online account. According to Suleyman (2017), some of the attackers will sell the email account that is been hacked to others to gain profit. It is important to protect our own account because our credit is priceless. It is hard to trace the attackers in the cyber world. The secure login system is needed to ensure the cybersafety. Therefore, this project would like to provide alternative ways to log in to a system because current login system is not secure enough..

B. Objective

The Main Purpose of this project is to provide security to enterprises using multiple level of authentication .Here we are using three level authentication system 1. Inserting user credentials to database 2.using RFID card 3. Face detection.

II. LITERATURE SURVEY

1) IEEE Xplore, three-level watchword Authentication System. This paper counsel the employment of every hardware token (smart card) and thus the software token (HOTP that's system generated). These 2 tokens are unit used as separate levels of authentication to form positive safety to the user profile
2) Implementation of Security System Exploitation 3- Level Authentication This paper can be a distinctive associate degree and mystic study of exploitation pattern as a watchword and implementation of a secured system, using three levels of security-(Text watchword, Pattern-Lock, and One-Time machine driven generated password).
3) IEEE Xplore, 4, April 2014, 3-Level watchword Authentication System. They planned a multifactor authentication theme that mixes the benefits of the current authentication schemes and thereby, overcomes the pitfalls of the presently used authentication schemes.
4) In 2018 Aparna M and Anjusree CM projected "Three level security system exploitation Image primarily based Authentication". This paper introduces OTP (one time watchword) construct password as their third level. They suggested exploitation image selection Authentication wherever user will choose explicit image from given choices as second level. Author has projected a special kinds of Authentication system, that area unit secured extremely.
5) In June, 2020 Rahul Chourasia projected "Three level watchword authentication system". This paper projected a mercantilism approach for matter content passwords. They suggested dynamical textual content passwords with the help of exploitation graphical passwords, that makes straightforward to remember and fewer troublesome for humans to use. In addition, the graphical word is bigger security.
6) In December, 2022 Gauri Sankar Mishra, Pradeep Kumar Mishra and Parmanand proposed "User Authentication: A 3 level password Authentication Mechanism". This paper relies on Users Authentication for Verification and Validation methodology. They proposed a technique wherever system verifies user if he or she claim to be by exploitation 3 level password verification

III. SOFTWARE/HARDWARE REQUIREMENTS

ESP 32 Development Board — ESP32 Development board is based on the ESP WROOM32 WIFI + BLE Module. It's a low-footprint, minimal system development board powered by the latest ESP-WROOM-32 module and can be easily inserted into a solderless breadboard. It contains the entire basic support circuitry for the ESP-WROOM-32, including the USB-UART bridge, reset- and boot-mode buttons, LDO regulator, and a micro-USB connector. Every important GPIO is available to the developer.

A. RFID Sensor

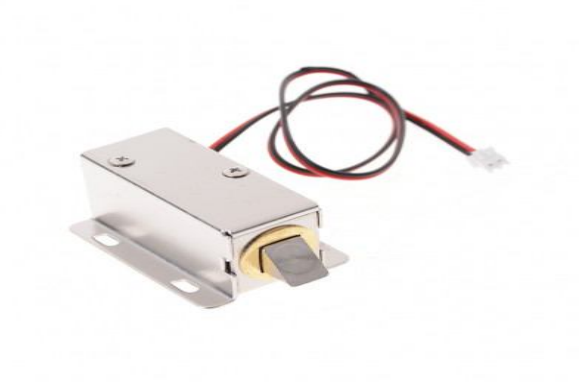
Rc522 - RFID reader/writer 13.56mhz with cards kit includes a 13.56mhz rf reader cum writer module that uses an rc522 ic and two s50 RFID cards. The mf rc522 is a highly integrated transmission module for contactless communication at 13.56 MHz. Rc522 supports iso 14443a/mifare mode.

Rc522 - RFID reader features an outstanding modulation and demodulation algorithm to serve effortless of communication at 13.56 MHz. The s50 RFID cards will ease up the process helping you to learn and add the 13.56 MHz rf transition to your project.

The module uses spi to communicate with microcontrollers. The open-hardware community already has a lot of projects exploiting the rc522 – RFID communication, using Arduino.

B. 12V Solenoid Electromagnetic Cabinet Door Lock

This DC 12V Solenoid Electromagnetic Cabinet Door Lock can be used for locking a sell-machine, storage shelves, file cabinets and etc. The hidden way of unlocking can be used for an emergency. The lock works as the circuit disconnects, and it will unlock as the instant power-on. It is steady, durable, and energy-saving and had a long lifespan. In the anti-theft and shockproof design, the lock is better than other kinds of locks. After connecting the wires and when the current is available, the electric lock can control the doors opening and closing.



C. LCD display

LCD (Liquid Crystal Display) is a type of flat panel display which uses liquid crystals in its primary form of operation. LEDs have a large and varying set of use cases for consumers and businesses, as they can be commonly found in smartphones, televisions, computer monitors and instrument panels. LCDs were a big leap in terms of the technology they replaced, which include light-emitting diode (LED) and gas-plasma displays. LCDs allowed displays to be much thinner than cathode ray tube (CRT) technology. LCDs consume much less power than LED and gas display displays because they work on the principle of blocking light rather than emitting it. Where an LED emits light, the liquid crystals in an LCD produces an image using a backlight.

IV. RESULT

Adding a smart card or pin, or a biometric factor can greatly increase security over the username and password, which can easily be gained through breaches or even simple social engineering. Advanced authentication helps to prevent a malicious party from spoofing the identity of a valid user to gain access to the system. Of course, fingerprints can be faked and smart cards can be stolen. There is no cure-all for network security, but using multiple factors for authentication to systems can minimize the threat greatlyadding a smart card or pin, or a biometric factor can greatly increase security over the username and password, which can easily be gained through breaches or even simple social engineering. Advanced authentication helps to prevent a malicious party from spoofing the identity of a valid user to gain access to the system. Of course, fingerprints can be faked and smart cards can be stolen. There is no cure-all for network security, but using multiple factors for authentication to systems can minimize the threat greatly

V. CONCLUSION

Three-level authentication system had been applied to the upper system which makes it extraordinarily secure at the facet of additional ease. This method can facilitate Man-in-the-middle attacks and Brute-force attacks on the user's side. A three-level security system could also be a protracted approach since the user should enter details rigorously for all 3 security levels and eventually, the user can add any image for its final level Authentications. Therefore, this method isn't appropriate for the overall purpose of security since it takes time to fill altogether three security-level details. but it'll undoubtedly be helpful in high-security levels wherever the protection of data could also be a concern and time quality is secondary

As a key element in facial imaging applications, such as facial recognition and face analysis, face detection creates various advantages for users, including the following:

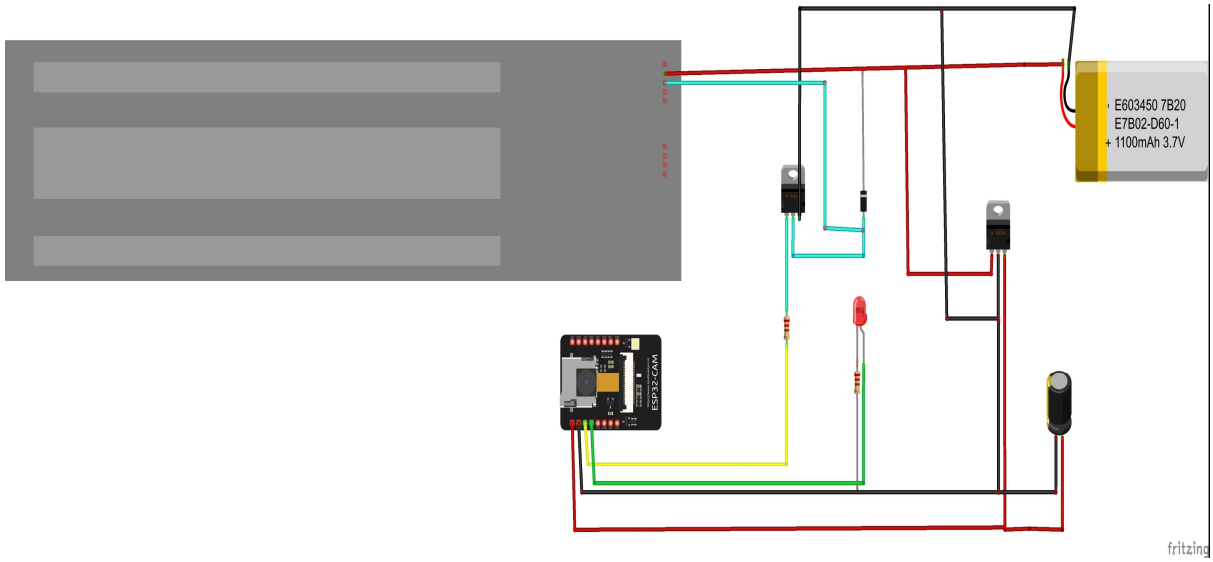
1) *Improved Security:* Face detection improves surveillance efforts and helps track down criminals and terrorists. Personal security is enhanced when users use their faces in place of passwords because there's nothing for hackers to steal or change.
2) *Easy to Integrate:* Face detection and facial recognition technology is easy to integrate, and most applications are compatible with the majority of cybersecurity software.
3) *Automated Identification:* In the past, identification was manually performed by a person; this was inefficient and frequently inaccurate. Face detection allows the identification process to be automated, saving time and increasing accuracy.

VI. FUTURE SCOPE

In the future, we tend to square measure able to add extra opinions like OTP (One Time Password) Authentication and Captcha Authentication wherever if the user uses VPN (Virtual non-public Network) to browse then multiple Captcha can stop the user to use the actual computer code package The most objective of this project is to boost the protection level of the systems for many survey papers where researched. It's found that a three-level authentication system helps to provide additional security compared to one-level and two-level authentication systems. three levels square measure additional important as a result of the user must enter vital details and log in with three utterly totally different levels of authentication.

We can also perform Face ID controlled Digital Door lock system using ESP32-CAM

The AI-Thinker ESP32-CAM module is a low-cost development board with a very small size OV2640 camera and a micro SD card slot. It has an ESP32 S chip with built-in Wi-Fi and Bluetooth connectivity, 2 high-performance 32-bit LX6 CPUs, 7-stage pipeline architecture



REFERENCES

[1] Abdurrahman, U. A., Kaiiali, M., & Muhammad, J., 2013. A new mobile-based multi-factor authentication scheme using pre-shared number, GPS location and time stamp. In: 2013 International Conference on Electronics, Computer and Computation, ICECCO 2013, 293–296. https://doi.org/10.1109/ICECCO.2013.6718286.

[2] Abo-Zahhad, M., Ahmed, S.M., Abbas, S.N., 2015. A new multi-level approach to EEG based human authentication using eye blinking. Pattern Recognit. Lett. 1–10. http://dx.doi.org/10.1016/j.patrec.2015.07.034.

[3] Chakraborty, N., Randhawa, G.S., Das, K., Mondal, S., 2016. MobSecure: a shoulder surfing safe login approach implemented on mobile device. Procedia Comput. Sci. 93 (September), 854–861. http://dx.doi.org/10.1016/j.procs.2016.07.256.

[4] Ding, D., Han, Q.-L., Xiang, Y., Ge, X., Zhang, X.-M., 2017. A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing. http://dx.doi.org/10.1016/j.neucom.2017.10.009

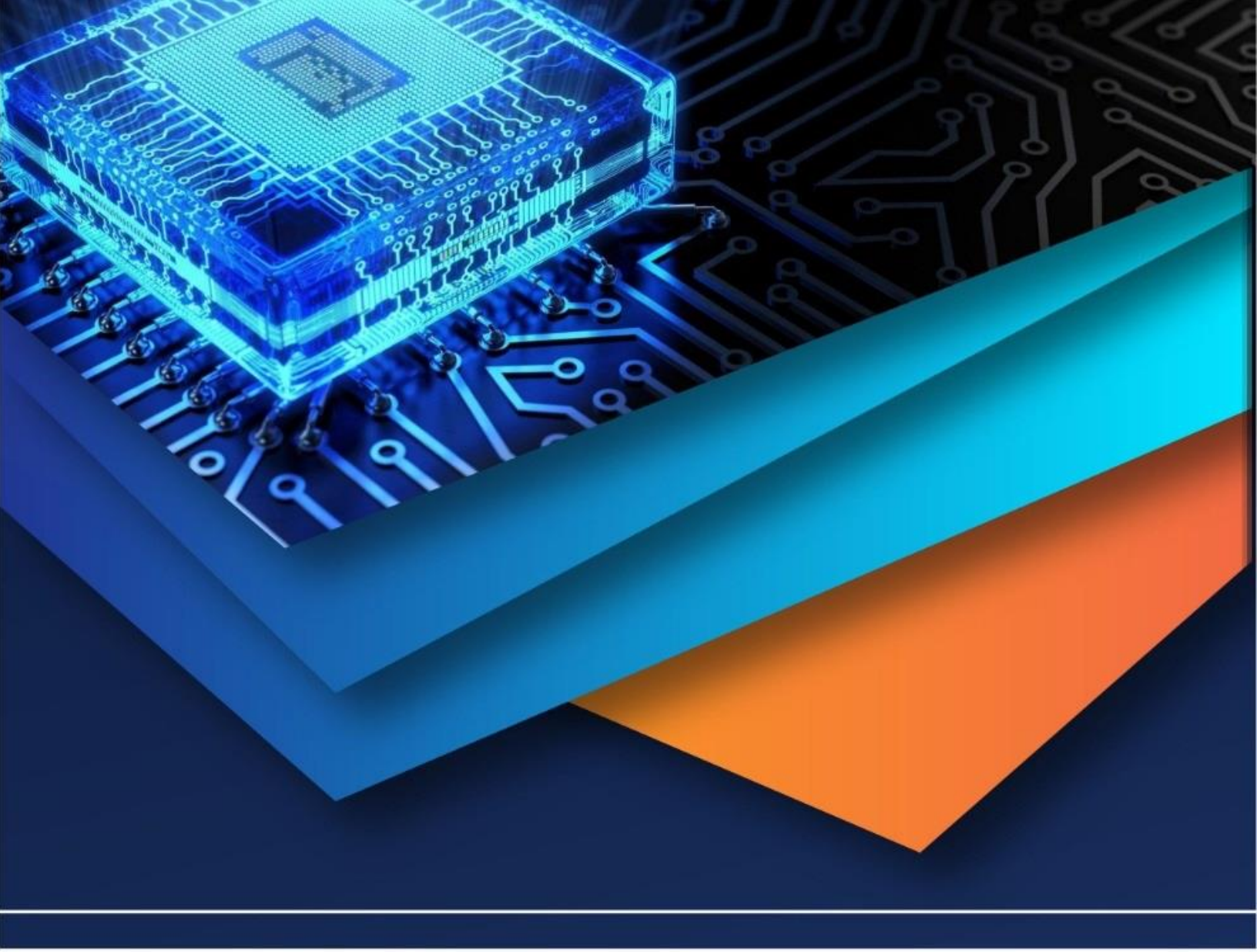
BIOGRAPHIES

Ashish Kumar
Student,
Dept. of Electronics and Telecommunication Engineering,
Sinhgad College of Engineering,
Maharashtra, India.

Abhinav Raj
Student,
Dept. of Electronics and Telecommunication Engineering,
Sinhgad College of Engineering,
Maharashtra, India.

Sourabh Suman
Student,
Dept. of Electronics and Telecommunication Engineering,
Sinhgad College of Engineering,
Maharashtra, India.

Prof. N.G BHOSKAR
Assistant Professor,
Dept. of Electronics and Telecommunication Engineering,
Sinhgad College of Engineering,
Maharashtra, India



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY