INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1463-1471

INTRUDER DETECTION AND EMAIL ALERTING SYSTEM

Godavarthy Sri Padma Praneeth[1], Chadarasi Bhavana Sai[2], Chakka Sravya[3], Chinthalapudi Bala Padmaja Praveena[4]

[1,2,3,4]Department of Information Technology, Shri Vishnu Engineering College for Women, Bhimavaram, Andhra Pradesh,534202, India.

ABSTRACT

This research paper introduces an Intruder Detection and Email Alerting System, designed to fortify user authentication and registration processes through the integration of face recognition technology within a web application framework. Leveraging Streamlit, a Python-based platform, and MySQL database management, the system offers a robust authentication mechanism with enhanced security features. Through facial recognition algorithms, user identities are verified during login, significantly reducing vulnerabilities associated with conventional password-based methods. Upon successful authentication, users gain access to system functionalities, including image capture and user registration. Intrusion attempts trigger immediate email notifications to system administrators, facilitating prompt response and heightened security vigilance. The paper presents the system's architecture, implementation details, and evaluation metrics, demonstrating its efficacy in safeguarding against unauthorized access. Additionally, future research avenues for expanding and refining the system's capabilities are discussed, underscoring its potential in diverse domains requiring stringent security measures.

1. INTRODUCTION

In recent years, the integration of advanced technologies has become imperative for enhancing security measures in various domains. One critical aspect of security is the protection of physical spaces, where the need for efficient intruder detection systems has grown significantly. This research paper presents a comprehensive study and implementation of an "Intruder Detection and Email Alerting System" employing the powerful combination of Streamlit and OpenCV technologies. Intrusion detection systems are pivotal in safeguarding premises against unauthorized access and potential security threats. The conventional methods often fall short in providing real-time monitoring and alerting capabilities, necessitating the exploration of innovative solutions. Leveraging the capabilities of computer vision and user-friendly web application frameworks, this project aims to deliver a robust and accessible system for intruder detection.The utilization of OpenCV, an open-source computer vision library, facilitates the development of sophisticated image and video processing algorithms. This enables the system to analyze live video feeds, recorded footage, identifying intruders.

2. LITERATURE SURVEY

A. INTELLIGENT ACOUSTIC AND VIBRATION RECOGNITION/ALERT

systems for detecting security breaches, identifying threats in close vicinity, and securing perimeters The development of systems that can identify potential dangers, such as individuals or vehicles approaching national properties, has been aided by an increasing emphasis on perimeter security, both domestically and internationally. Integrating numerous sensors—each with unique modalities and detection ranges—to produce a versatile and reliable device is one area of focus. They suggest a gadget that provides security threat detection and categorization, and it is built around three security sensors that have been shown to work. In particular, these sensors are vibration, seismic, and acoustic. The "Smart Fence" gadget based on these sensors will be especially useful for the identification and reporting of successive approaching situations, such as an approaching car with people intending to breach a gated site. Long-distance cars, for example, might pose less of a hazard than someone breaking into a secure perimeter, who might pose less of a concern than someone trying to scale a barrier surrounding the perimeter. The interesting auditory fingerprints emitted by approaching humans and moving vehicles are intricate. They propose utilizing an algorithm motivated by neurobiology to identify automobiles that are approaching and to classify the type of vehicles. Unsupervised learning with an unknown audio signature is accomplished by nonlinear Hebbian learning (NHL), a straightforward and visually appealing neural learning mechanism present in the human brain. Three categories of vehicles can be distinguished by the established system: light track, heavy track, and motorbike. The purpose of a seismic based human danger detector is to distinguish approaching humans and to differentiate between the series of events caused by the animal and the history of passenger vehicles and a single vibration occurrence, such as the collapse of a tree limb. The sensor employed was a geophone-based seismometer, which is a low-cost device with the ability to detect large distances and provide easy and quick deployment. Gaussian mixture models were created to

characterize statistical aspects of the temporal gait and frequency data collected from the seismic signals. The system was set up to differentiate between human footfall, autos, and backgrounds. To detect and classify fence breaches, a 3-axis accelerometer has been employed. The developed method based on a non-homogeneous Markov model is able to identify the type of breach, whether it is the result of someone climbing on the fence or a strong wind rattling the barrier. The suggested algorithm and gadget have been tested on several fences and have demonstrated reliable detection for differentiating between climb,kick, rattle and context.

B. INTRUSION DETECTION SYSTEMS (IDSS) WITH LOW POWER ACCELEROMETER-BASED TAMPER AND INTRUSION DETECTION SYSTEMS

employ a variety of sensors to detect illicit attempts to access restricted areas and to provide alerts to security response teams. The main sensor technologies for interior safety are magnetic switches, microwave sensors, video detectors, proximity sensors, and passive infrared (PIR) sensors. In this research, another sensory modality is employed: since most incursions result in vibrations, it is possible to perceive these vibrations and build a detector. The suggested sensor may also be utilised for tamper detection if the vibration caused by the attack can be used to identify the unapproved movement of things that are protected. Because they don't require wiring or cabling, wireless sensors are more convenient to deploy than their wired counterparts. For wired detectors, power may be supplied with ease; however, power efficiency is a crucial design consideration for wireless sensors.Duty-cycling reduces a sensor's power usage by having it operate for a brief while before shutting off for another period of time to conserve electricity. In comparison to awake time, more energy can be saved the longer one sleeps. Naturally, sensors need to be able to sense, therefore they need to stay awake for a certain amount of time. In this research, a novel sensor that expands the sensor's low-energy operation capabilities is proposed. It uses affordable MEMS accelerometers in conjunction with a basic mechanical system. When duty-cycling is applied, the interval between two sensor awakenings must be negligibly less than the length of the event that has to be detected. The possible duty cycle is limited by this reality, given an event shape.The duration of the vibration caused by different acts must be considered because the suggested approach uses vibrations to identify undesired attempts. In our suggested solution, however, we employ a hardware extension of the sensor that extends the event's influence over time, permitting reduced duty cycles and lower energy consumption. The new energy-efficient MEMS accelerometer-based sensor that is proposed in this research can be employed as a temperature or intrusion detector. The sensor's basic component is a low-cost BMA180 accelerometer, which can be extended mechanically to lengthen time events and reduce duty cycle activity. In performance tests, the suggested sensor fared remarkably well (100 percent hit rate) with service cycles as low as 5–10 percent. The sensor can be utilised wirelessly because to its low power consumption.

C. SECURING IOT DEVICES AND SECURELY CONNECTING THE DOTS USING REST API AND MIDDLEWARE

The Internet of Things allows data transmission and reception by connecting computing devices that are integrated into common objects to the Internet. The first is that by processing the data, we can reduce waste, failure, and expense. The second is that we can empower our machines to collect environmental data without the need for human intervention. Digital and real worlds can talk to each other thanks to the Internet of Things. The digital and physical worlds can communicate thanks to sensors and actuators. These sensors collect data that must be processed, stored, and examined. On a distant server or in the cloud, data processing might occur at the edge of the network. The resources available to an IoT item determine its processing and storage capabilities, which are restricted by size, energy, power and computational capacity. As a result, these systems depend on IoT middleware to provide the necessary functionality.

D. SECURITY AND PRIVACY OF SMART HOME SYSTEMS BASED ON THE INTERNET OF THINGS AND STEREO MATCHING ALGORITHMS

The Internet of Things allows data transmission and reception by connecting computing devices that are integrated into common objects to the Internet. The first is that by processing the data, we can reduce waste, failure, and expense. The second is that we can empower our machines to collect environmental data without the need for human intervention. Digital and real worlds can talk to each other thanks to the Internet of Things. The digital and physical worlds can communicate thanks to sensors and actuators. These sensors collect data that must be processed, stored, and examined. On a distant server or in the cloud, data processing might occur at the edge of the network. The resources available to an IoT item determine its processing and storage capabilities, which are restricted. In this field, there's still a lot of space for innovation, even though some technologies are pretty mature. Internet of Things (IoT)-focused smart home systems have unavoidably emerged as a hotbed of research in recent years. Because of this, this article explores the hardware and software viability of designing smart home devices. By building the application of

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1463-1471

an IoT module, the device information is precisely analyzed and monitored using the stereo matching method. The entire architecture of the system has been reinforced, guaranteeing the safety and intelligence of users' residences while simultaneously promoting the development of smart houses.

E.IOT BASED SMART HOME SURVEILLANCE AND AUTOMATION

Protection of living things has become crucial for modern lifestyles since it is difficult to oversee monitoring and surveillance seven days a week, twenty-four hours a day. Utilizing the newest technology in Internet of Things applications is one of the finest choices. Using IoT, we can obtain information about potential security threats, damage and danger alarms, and extra controls over home equipment for convenience, automation, and home security. The Raspberry Pi board controls and keeps an eye on the futuristic sensors and sensing transducers for automation and surveillance. A "smart home" is one that has advanced automated systems pre-programmed to handle various activities, such opening and closing doors and windows, detecting gas leaks, and detecting fires, among other things. With smartphones becoming more affordable and user-friendly, home automation is also growing. due to the widespread use of numerous cutting-edge wireless communication techniques and technologies (GSM, WIFI, Bluetooth). One technology that has the power to change a user's lifestyle is the Internet of Things (IoT). In other words, the internet has altered how we interact with people online and conduct business. With the Internet of Things, you may communicate with the electrical and electronic equipment in your house from any location. We may now operate and watch the household appliance at our convenience thanks to the advancement of knowledge, such as the Raspberry Pi.

F. DETERMINING DAMAGE ACTIVITIES FOR SECURITY AROUND THE PERIPHERY

Perimeter security for the home, the country's border, the airport, the military installation, the transportation hub, and the pipelines carrying oil and gas, among other things, has recently come under increased national and individual scrutiny. The following features should be included in a perimeter protection system: 1) it should be able to track in real time throughout the day in all weather conditions and relay signals over long distances; 2) it should be intelligently sensitive to the environment so that it can distinguish between routine and dangerous activities with ease; and 3) it should be able to adapt to new environmental changes. Conventional perimeter defence systems use ultrasonic, microwave, infrared, or photoelectric sensors to detect intruders. These sensors have a restricted detection range, though, because they require power. Since the development of fibre sensor technology, perimeter security has effectively employed fibre sensors. Compared to other sensors, fibre sensors are more advantageous because to their straightforward design, low cost, capacity to communicate over long distances, precise positioning, and energy efficiency. It can convey signals and sense the atmosphere as well. A fiber-based perimeter security system has been created. Unfortunately, the system lacks the intelligence to determine what kind of destructive action has taken place. Wang provides a fiber-sensor based long-range safety monitoring system for underground oil pipelines. He studies vibration signals as well. But only frequency data is considered, and the list of dangerous behaviours is limited to three types. Building on our earlier research [7, 8], the focus of this paper is on enhancing the intelligence of the perimeter security system—that is, enabling it to identify more risky activity. Using vibration signals acquired from a fibre sensor as data source, we perform statistical analysis using Gram-Charlier series and time-frequency analysis by wavelet packet decomposition to create a feature vector of each vibration signal fragment. Since there are signals for which there are no optimal wavelet packet bases, we propose a technique to determine the second best wavelet packet bases. Independent component analysis (ICA) is used for de-correlation. An SVM tree technique based on kernel space hierarchical clustering is also described for the classification process. It has been shown that the suggested feature extraction classification approach, which uses vibration signals from fibre sensors to identify destructive actions, is effective.We will conduct in-depth studies on novel types of risky behaviour in the future. In addition, the vibration signals emitted by different kinds of activities exhibit a number of unique time domain evolution properties, including vibration signal length and trend. There's been some underuse of this type of character, which is something to take into account. Furthermore, we can train for possible real-world applications using online incremental learning.

G. ALERT INTRUDER DETECTION SYSTEM USING PASSIVE INFRARED MOTION DETECTOR BASED ON INTERNET OF THINGS

The implementation of Internet of Things (IoT) in various domains has garnered significant attention, with a focus on enhancing daily life through connected devices. One crucial aspect involves the integration of IoT into home security systems, particularly in the context of intruder detection. The following literature review delves into existing research related to intruder detection systems using Passive Infrared Motion Detectors (PIR) based on IoT. Several studies have explored the integration of IoT for intruder detection, with a common emphasis on the challenges posed by resource-constrained devices. The unique characteristics of IoT devices necessitate innovative approaches to implement motion

detection techniques effectively. The use of Passive Infrared Motion Detectors stands out as a promising solution, leveraging the technology to enhance home security. The existing literature lie in the exploration of IoT's potential in home security, offering a range of benefits. The use of Passive Infrared Motion Detectors is identified as effective for detecting intruders, providing automated motion detection in various scenarios. However, limitations revolve around the resource constraints of IoT devices, posing challenges in terms of implementation complexity and potential false positives or negatives. The literature revolve around the need for more in-depth exploration of the limitations associated with Passive Infrared Motion Detectors in real-world scenarios. Additionally, there is a lack of consensus on the optimal methodologies for integrating IoT and motion detection systems, leading to varied approaches and outcomes in different studies. Collectively, the literature suggests a growing trend towards utilizing Passive Infrared Motion Detectors in IoT-based intruder detection systems. Common consensus acknowledges the effectiveness of this technology, albeit with variations in implementation methodologies. The need for standardized approaches and a deeper understanding of real-world limitations emerges as a pattern requiring further exploration.

H. SAFE ENTRY, EASY EXIT

The escalating frequency of violent incidents in educational institutions has prompted a sustained focus on bolstering security measures in schools and universities. Of particular concern is the vulnerability associated with access points, with doors emerging as critical elements in ensuring the safety of students, faculty, and staff. This literature review explores existing research and strategies aimed at enhancing school security, focusing on well-designed doors supplemented by advanced equipment to thwart intruders, control access, and prevent damage. Numerous studies underscore the importance of addressing security concerns in educational facilities, emphasizing the pivotal role that doors play in fortifying the overall security infrastructure. The consensus is that schools require doors that strike a delicate balance – facilitating entry for authorized individuals while effectively preventing unauthorized access. The literature consistently advocates for a comprehensive approach, combining robust door designs with supplementary equipment to create a secure environment conducive to learning. The literature primarily revolve around the acknowledgment of doors as critical security elements and the advocacy for a holistic security strategy. Well-designed doors, when properly secured, are deemed effective in controlling access and preventing unauthorized entry. However, weaknesses lie in the lack of a universal standard for school security measures, resulting in variations in implementation across institutions. Additionally, challenges related to the cost and maintenance of advanced security systems are recurrent themes. A noticeable gap in the literature pertains to the need for empirical studies assessing the effectiveness of specific door designs and security strategies in diverse educational settings. The lack of standardized guidelines and best practices for implementing security measures tailored to individual school contexts is a limitation. Contradictions arise in the divergent opinions on the extent of technological integration, with some advocating for cutting-edge solutions and others emphasizing the importance of simplicity and ease of use.

I. RASPBERRY PI BASED INTRUDER DETECTION WITH IMAGE EMAIL ALERT THOUGH IOT

An efficient, low-cost embedded access control system for smart home security and remote monitoring is crucial for various commercial and security applications. The IoT has spurred the adoption of smart home security control systems, leveraging interconnected devices to enhance surveillance capabilities. Researchers are developing frameworks to enable users to interact with appliances through separate user interface devices, such as smartphones, addressing usability challenges.Existing literature showcases contributions in IoT-enabled home security systems. Rani et al. (2018) proposed an IoT-based system using Raspberry Pi for SMS alerts and email notifications of unauthorized individuals. Dinakar et al. (2018) introduced an IoT-based automated security system for intruder detection . Ghodke et al. (2017) presented an IoT network-based system for home security image alerts. Anwar et al. (2016) described an IoT-based door accessibility system with smartphone voice alerts . Tanaya and Kishore (2016) upgraded home security with face detection techniques, while Chowdhury et al. (2013) developed an IoT-based access control system using Raspberry Pi . Common components include PIR sensors for motion detection and Pi Cameras for image capture, with limited research on human face and object detection algorithms. However, advancements in image processing offer promise for enhancing surveillance capabilities. In summary, IoT-enabled home security systems offer 24/7 monitoring, real-time alerts, cost-effectiveness, and precise notifications. Further research in this area can drive innovation to meet evolving security needs.

J. GPS BASED AUTOMATIC IMAGE CAPTURING AND EMAIL ALERTING SYSTEM

The integration of GPS with automatic image capture and email alert systems advances surveillance and security. Previous studies enhance traditional systems with GPS for precise geolocation. This approach finds applications in asset tracking and fleet management, showcasing GPS versatility. The proposed system augments security by combining GPS modules with image capture and email protocols. Key aspects include sensor selection, data

processing, and communication. Research explores sensor technologies like PIR and ultrasonic sensors, alongside image processing for automated intrusion detection. Moreover, email alerts promptly notify stakeholders of security breaches, enabling remote monitoring and response. This system offers improved security and peace of mind. Future work may optimize performance and address cyber security concerns for broader adoption. Overall, the proposed GPS-based automatic image capturing and email alerting system represents a significant advancement in surveillance technology, offering enhanced security and peace of mind for users. Future research in this area may focus on optimizing system performance, expanding functionality, and addressing potential cyber security concerns to ensure the widespread adoption and effectiveness of such systems in various settings.

K. KEYLESS ACCESS

The security of physical spaces hinges on the fundamental truth that a misplaced key can compromise the protective armor against unwelcome intruders. In the context of large universities, where the distribution and retrieval of thousands of keys present significant challenges, administrators and security officials grapple with the need for efficient access-control solutions. This literature review explores existing research and strategies related to keyless access-control systems, particularly those utilizing swipe or contactless cards, to secure campus facilities. Numerous studies emphasize the vulnerabilities associated with traditional lock-and-key systems, underscoring the imperative for advanced access-control solutions. The appeal of keyless access-control systems has grown steadily, primarily driven by technological advancements that enable swipe or contactless card functionalities. The central argument is that such systems enhance security, mitigate the risks associated with lost keys, and offer administrators greater control over access to campus facilities. The literature revolve around the acknowledged benefits of keyless access-control systems. These systems are praised for providing secure and convenient access, reducing the administrative burden of managing physical keys, and offering scalability for large campuses. However, weaknesses include the potential for system incompatibility when different departments independently adopt disparate access-control solutions, leading to challenges in achieving uniform security standards across the entire campus. A notable gap in the literature pertains to the need for standardized guidelines and best practices for implementing keyless access-control systems in large and diverse university settings. Contradictions arise in the challenges posed by the coexistence of traditional lock-and-key systems alongside modern access-control technologies, resulting in fragmented security infrastructures. Limitations include the potential for technological obsolescence and the necessity for comprehensive training programs to ensure effective utilization.

S No.	Paper title	Technologies used	Strengths	Weakness
1.	INTELLIGENT ACOUSTIC AND VIBRATION RECOGNITION/ALERT	Vibration sensor and Seismic sensor	Versatality Reliability	Sensitivity to environmental factors Complexity
2.	INTRUSION DETECTION SYSTEMS (IDSS) WITH LOW POWER ACCELEROMETER-BASED TAMPER AND INTRUSION DETECTION SYSTEMS	MEMS Accelerometers	Low Power Consumption Wireless deployment	Mechanical Extension Complexity Event Duration Limitations
3.	SECURING IOT DEVICES AND SECURELY CONNECTING THE DOTS USING REST API AND MIDDLEWARE	Internet of Things (IoT) Devices RESTful APIs	Efficient Data Processing Automation and Remote Monitoring	Security Risks Complexity and Compatability
4.	SECURITY AND PRIVACY OF SMART HOME SYSTEMS BASED ON THE INTERNET OF THINGS AND STEREO	Internet of Things (IoT) Stereo Matching Algorithms	Enhanced Data Processing Improved Safety and Intelligence	Privacy Concerns Complexity and Cost

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1463-1471

	MATCHING ALGORIHMS			
5.	IOT BASED SMART HOME SURVEILLANCE AND AUTOMATION	Internet of Things (IoT) Raspberry Pi	Enhanced Home Security Convenience and Automation	Reliance on Internet Connectivity Security Risks
6.	DETERMINING DAMAGE ACTIVITIES FOR SECURITY AROUND THE PERIPHERY	Fibre sensor technology	Long-Range Monitoring Energy Efficiency	Limited Intelligence Scope of Detected Behaviors
7.	ALERT INTRUDER DETECTION SYSTEM USING PASSIVE INFRARED MOTION DETECTOR BASED ON INTERNET OF THINGS	Passive Infrared Motion Detectors (PIR)	Effective Intruder Detection Integration with IoT	Resource Constraints False Positives/Negatives
8.	SAFE ENTRY, EASY EXIT	Advanced Door Designs Supplementary Security Equipment	Effective Access Control Comprehensive Security Infrastructure	Lack of Universal Standards Cost and Maintenance Challenges Limited Empirical Studies
9.	RASPBERRY PI BASED INTRUDER DETECTION WITH IMAGE EMAIL ALERT THOUGH IOT	Raspberry Pi Passive Infrared (PIR) Sensors Internet of Things (IoT) Pi Camera	24/7 Monitoring Real-time Alerts	Limited Face and Object Detection Usability Challenges
10.	GPS BASED AUTOMATIC IMAGE CAPTURING AND EMAIL ALERTING SYSTEM	Global Positioning System (GPS) Image Capture Sensors	Enhanced Security Remote Monitoring and Response	Dependency on Network Connectivity Potential Cybersecurity Risks
11.	KEYLESS ACCESS	Keyless Access-Control Systems	Enhanced Security Convenience and Efficiency	System Compatibility Technological Obsolescence

3. METHODOLOGIES

1. User Authentication:

Database Integration: Utilizing MySQL as the backend database management system for storing user credentials and related information.

SQL Queries: Employing SQL queries to interact with the database, including user authentication by checking username and password against stored records.

2. Face Recognition:

Library Selection: Choosing the face_recognition library, which provides a high-level interface for face recognition tasks.

Image Processing: Capturing images from the camera using OpenCV and processing them for face recognition.

Algorithm Implementation: Implementing face recognition algorithms to compare the captured image with images stored in the database.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

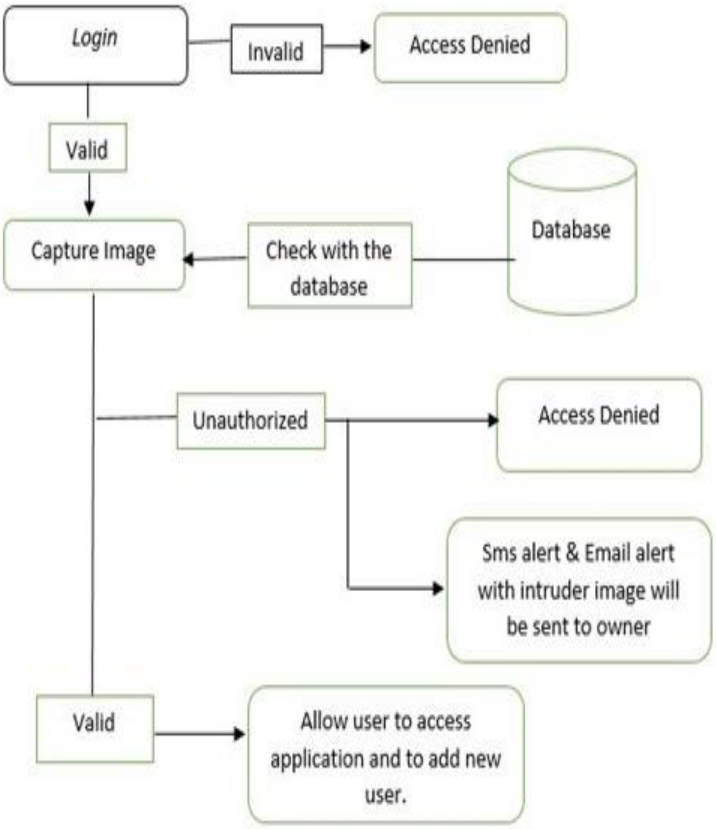
Vol. 04, Issue 05, May 2024, pp: 1463-1471

3. Sending Alerts :

Email Notification: When unauthorized access is detected, the code sends an email alert using SMTP. It constructs an email message with a subject, body, and attached image file and sends it using Gmail SMTP server.

SMS Notification : The code sends an SMS alert using the Twilio API when unauthorized access is detected. It constructs a message body and sends it to a specified recipient phone number using the Twilio REST API.

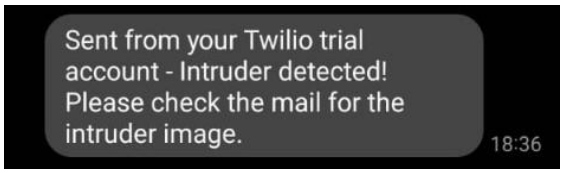
4.Adding New Users: After successful login and authorization, the user can add new users to the system. The code allows users to input a new username, password, email, and upload an image. It then inserts the user's information into the MySQL database.



5. Session Management: The code uses Streamlit's session state to keep track of whether the user has been authorized via image recognition. This allows access to additional functionalities, such as adding new users, only after successful authorization.

4. RESULTS

The project is a robust authentication system utilizing facial recognition technology alongside conventional username and password authentication. Users first input their credentials, and upon successful login, the system captures an image from the webcam. This captured image is then compared against a reference image stored in the database, using the face recognition library. If the comparison yields a match within a specified tolerance level, access is granted. However, if the captured image doesn't contain a recognizable face or the face doesn't match the stored image, indicating unauthorized access, the system triggers a series of notifications. It sends an email alert with the captured image attached, informing administrators or authorized personnel of the security breach.Additionally, it sends an SMS alert via Twilio to ensure immediate attention to the unauthorized access attempt. Authorized users also have the capability to add new users to the system, providing details such as username, password, email, and uploading an image for future recognition. Throughout the process, robust error handling ensures the system remains operational even in the event of unexpected errors, ensuring reliability and security in user authentication and access management.



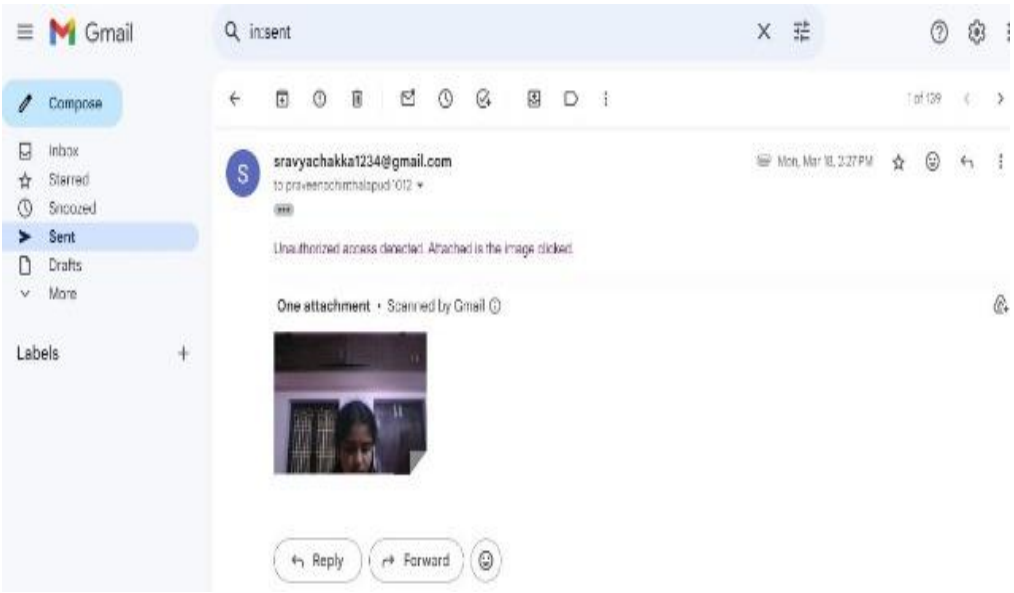
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1463-1471



5. CONCLUSION

In conclusion, the development and implementation of the Intruder Detection and Alerting System represent a significant advancement in enhancing user authentication and security within web applications. By integrating face recognition technology with Streamlit and MySQL database management, the system provides a robust and efficient authentication mechanism that mitigates the vulnerabilities associated with traditional password-based methods.

Through real-time facial recognition algorithms, users are authenticated with a high degree of accuracy, ensuring only authorized individuals gain access to the system's functionalities. The incorporation of image capture capabilities further enhances security measures, allowing administrators to monitor and respond promptly to unauthorized access attempts.

The system's ability to send immediate email notifications upon detecting intrusions provides administrators with timely alerts, enabling swift action to mitigate security breaches and safeguard sensitive information. Moreover, the user-friendly interface of the application streamlines the registration process for adding new users, facilitating seamless integration into existing systems.

Overall, the Intruder Detection and Alerting System offer a comprehensive solution for bolstering security measures in web applications, demonstrating its effectiveness in protecting against unauthorized access and ensuring user data integrity. As advancements in facial recognition technology continue to evolve, future iterations of the system hold promise for further enhancing security protocols and meeting the evolving demands of the digital landscape.

ACKNOWLEDGEMENTS

We would like to express our sincere gratitude to our college administration for providing us with the necessary resources and infrastructure to carry out this project. We extend our heartfelt thanks to Shri Vishnu Engineering College for Women for fostering an environment of innovation and learning.

We are deeply grateful to our esteemed Principal, G.Srinivasa Rao, for his/her unwavering support and encouragement throughout our academic journey. His/her guidance has been invaluable in shaping our project and nurturing our passion for technology.

We also extend our appreciation to P.Srinivasa Raju, whose support and mentorship have been instrumental in our project's success. His/her dedication to academic excellence has inspired us to strive for greatness in all our endeavors.

Our sincere thanks to Dr.D.V.Naga Raju, Head of the Department of Information Technology, for his/her guidance and support in navigating the academic challenges of our project. His/her expertise and wisdom have been invaluable in guiding us towards our goals. We would like to express our gratitude to our mentor, Dr.D.V.Naga Raju, for his/her invaluable guidance, encouragement, and support throughout the duration of this project. His/her expertise and insights have been instrumental in shaping our project and pushing us to achieve our full potential.

Finally, we would like to thank all our classmates, friends, and family members for their unwavering support and encouragement throughout this journey. Their constant encouragement and belief in our abilities have been a source of strength and motivation.

6. REFERENCES

[1] M. Andriansyah, M. Subali, I. Purwanto, S. A. Irianto and R. A.Pramono, ”e-KTP as the basis of home security system using arduino UNO,” 2017 4th International Conference on Computer Application And Information Processing Technology (CAIPT), Kuta Bali, 2017, pp.1-5 .

[2] A. A. Dibazar, A. Yousefi, H. O. Park, B. Lu, S. George and T. W. Berger, ”Intelligent acoustic and vibration recognition/alert systems for security breaching detection, close proximity danger identification, and perimeter protection,” 2010.

[3] IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, 2010, pp. 351-356, doi: 10.1109/THS.2010.5654931.

[4] G. Vakulya and G. Simon, ”Low power accelerometer based intrusion and tamper detector,” 2014 IEEE 11th International Multi-Conference on Systems, Signals Devices (SSD14), Barcelona, Spain, 2014, pp. 1-6, doi: 10.1109/SSD.2014.6808878.

[5] Iyer Saikumar, Gaonkar Pranjal, Wadekar Shweta, Kohmaria Nayan and Upadhyay Prashant, IoT based Intruder Detection System Using GSM (April 8, 2020). Proceedings of the 3rd International Conference on Advances in Science Technology (ICAST) 2020, Available at SSRN: https://ssrn.com/abstract=3572326 or http://dx.doi.org/10.2139/ssrn.3572326.

[6] Zhengbing Hu, V. Nimko and P. Bykovyy, ”Fuzzy logic based method to estimate the risk of alarm system false detection,” Proceedings of International Conference on Modern Problem of Radio Engineering, Telecommunications and Computer Science, Lviv, UKraine, 2012, pp. 452-453

[7] H. Yan, G. Shi, Q. Wang and S. Hao, ”Identification of Damaging Activities for Perimeter Security,” 2009 International Conference on Signal Processing Systems, Singapore, 2009, pp. 162-166, doi: 10.1109/ICSPS.2009.17 [7] A Anitha, “Home security system using internet of things” 2017 IOP Conf. Ser.: Mater. Sci. Eng.263 042026