MACHINE LEARNING BASED SECURITY SYSTEM FOR OFFICE PREMISES

Abstract: Safety plays a major role in today's world. User authentication, i.e., a procedure to verify the identity of the user, is essential in the digital world so as to protect the user's personal data stored online (e.g. online bank accounts) and on personal devices (e.g., smart phones, laptops) and to also enable customized services in smart spaces (e.g., adjusting room temperature etc.). Recently, traditional authentication mechanisms (e.g., passwords or fingerprints) have been repeatedly shown to be vulnerable to subversion. Researchers thus have proposed numerous new mechanisms to authenticate the users in the aforementioned scenarios. At offices and work places as well, this user authentication is of utmost importance in order to avoid any mal-practices if any as well as to maintain individual work privacy in the organization. This project aims at developing a user authentication system for offices based on their company generated login ID and passwords, One-Time-Password (OTP) generation and face recognition. The system also has features such as auto-saving data to server and auto-logout.

Keywords: AutoSaved, Auto-logout, Face recognition, Login ID and passwords credentials, One-Time-Password (OTP).

I. INTRODUCTION

Currently systems are protected using many firewalls, IDS and security software. The existing system can be easily compromised by any tool used by attacker. The aim of system is to provide effective authentication from unauthorized users by providing three tier authentications which are login credentials, face Recognition scanner and OTP. The proposed methodology provides more control over data stored in system by restricting the access to specific user for specific file with limited privileges and for limited time period on the basis of secret key authentication using symmetric as well as asymmetric mechanism. The integrity and confidentiality of data is fully guaranteed by not only encrypting the data using secret key but also to the access permission and limited file information. Especially, the purpose of the one-time password is to make it more difficult to gain unauthorized access to restricted resources.

The authentication, confidentiality and privacy of data is needed in today's world. The smart devices, like smart phones and sensing nodes, are now developing an emerging global and Internet-based information service platform called the Internet of Things (IoT). Generally, the IoT architecture is based on some existing data communication tools, which could range from RFID (Radio Frequency Identification) -tagged products to complex computational items. Due to the inherent vulnerabilities of the Internet, security and privacy issues should be considered and addressed before the Internet of Things is widely deployed. Direct interaction of smart devices within the immediate living space of humans intimidates new security vulnerabilities. Research has been led in developing customized tools for computer security to establish confidentiality, integrity and availability. In case of any kind of security failure, our system provides the users data fully data security and assurance of privacy. The aim is to prevention system that is adaptive and receptive to new threats and provides more control of owner on the data stored on system by restricting the access to particular user for specific file with limited rights. The idea behind it to create software that will protect the data from all kinds of attacks and maintain entire confidentiality of the data.

II. LITERATURE REVIEW

There has been a use of three tire architecture in paper "Effective Authentication For Restricing Unauthorized User", [1] for providing security to the system. Those tiers are Facial recognition, Fingerprint Scanning and OTP. All these tiers give a great strength to security of system. Incase if there is an attack on system, the measures are provided so as to not leak the important data from the system. By using AES 512 all the data is encrypted which can only be decrypted by a specific key.

The security and protection of such personal information are becoming more and more important since mobile devices are vulnerable to unauthorized access or theft. User authentication is a task of paramount importance that grants access to legitimate users at the point-of-entry and continuously through the usage session. This task is made possible with today's smartphones' embedded sensors that enable continuous and implicit user authentication by capturing behavioral biometrics and traits. In [2], Mohammed Abuhamad et al surveyed more than 140 recent behavioral biometric-based approaches for continuous user authentication, including motionbased methods, gait-based methods, keystroke dynamics-based methods, touch gesturebased methods, voice-based methods (16 studies), and multimodal-based methods. The survey provides an overview of the current state-of-the-art approaches for continuous user authentication using behavioral biometrics captured by smartphones' embedded sensors, including insights and open challenges for adoption, usability, and performance.

Biometric authentication of an individual through their own characteristics is the most common way to identify a person. In [3], a multimodal biometric user verification system with identical twin shows the fingerprint, face and lip classification model using SVM2 with kernel functions is efficient and promising. It would be seen from the results that the FRR is less than that of FAR.

Paper "Multi-Biometric Authentication Using Deep Learning Classifier for Securing of Healthcare Data "[4] analyzes the performance of combining the use of on-line signature and fingerprint authentication to perform robust user authentication. Signatures are verified using the dynamic time warping (DTW) technique of string matching. The proposed minutiae-based matching algorithm, stores merely a small number of minutiae points, which greatly reduces the storage requirement with the help of phase correlation. Here, matching score level fusion is used by applying weighted sum rule for the biometric fusion process. To improve the authentication performance, deep learning classifier is proposed in this work for multi-biometrics authentication. When a biometric authentication request is submitted, the proposed authentication system uses deep learning to automatically select an appropriate matching image. In the experiment, biometric authentication was performed on healthcare in the UCI database. Multi -Biometric Authentication was used during the authentication stage.

Presently a-days Cloud registering is rising field in light of its Performance, high accessibility, easily. Information store is principle future that cloud benefit gives to the huge association to store tremendous measure of information. Yet at the same time numerous associations are not prepared to execute distributed computing innovation since absence of security. So the principle goal of [5] is to understand the security issues and to anticipate unapproved access in distributed storage, it should be possible with the assistance of an effective validation strategy by utilizing cross breed verification calculation to give security of the information in cloud and guarantee amending code to keep up the nature of administration. In any case, solid client confirmation that confines illicit access to the administration giving servers is the foremost prerequisite for securing cloud condition

Authentication of a user through an ID and password is generally done at the start of a session. But the continuous authentication system observes the genuineness of the user throughout the entire session, and not at login only. In [6], Suhail Javed Quraishi and Sarabjeet Singh Bedi proposed the usage of keystroke dynamics as biometric trait for continuous user authentication in desktop platform. Biometric Authentication involves mainly three phases named as enrollment phase, verification phase and identification phase. The identification phase marks the accessed user as an authenticated only if the input pattern matches with the profile pattern otherwise the system is logout. The proposed Continuous User Biometric Authentication (CUBA) System is based on free text input from keyboard. There is no restriction on input data during Enrolment, Verification, and Identification phase. Unsupervised One-class Support Vector Machine is used to classify the authenticated user's input from all the other inputs. This continuous authentication system can be used in many areas like in Un-proctored online examination systems, Intrusion & Fraud Detection Systems, Areas where user alertness is required for entire period e.g. Controlling Air Traffic etc

The significant growth in users of e-learning technologies and their use in courses have given rise to a major concern over protecting them from misuse; a significant concern is that of the potential for cheating or illicit assistance during online

examinations. Paper “A Robust e-Invigilation System Employing Multimodal Biometric Authentication”, presents the development of robust, flexible, transparent and continuous authentication mechanism for e-assessments. To monitor the exam taker and ensure that only the legitimate student is taking the exam, the system offers a continuous user identification employing multimodal biometrics; a security layer using an eye tracker to record the student’s eye movement; and, speech recognition to detect inappropriate communication. The focus of [7] in particular is the development and evaluation of 3D facial authentication. An experiment has been conducted to investigate the ability of the proposed platform to detect any cheating attempts. During the experiment, participants' biometric data, eye movement, and head movements have been collected using custom software. The 3D camera also captured the session using a built-in microphone and the system recognized speech (employing a speech recognition algorithm). 51 participants participated in this experiment. The FRR of all legitimate participants was 0 and 0.0063 in 2D and 3D facial recognition modes respectively. Furthermore, three participants were tasked with a series of eight scenarios that map to typical misuse. The results of the FAR and FRR of five of these threat scenarios in both 2D and 3D mode were 0 with two cases exhibiting an FAR of 0.11 and 0.076 in the 2D mode.

Currently systems are protected using many firewalls, IDS and security software. The existing system can be easily compromised by any tool used by attacker. The aim of system is to provide effective authentication from unauthorized users by providing two tier authentications which are Irish Recognition scanner and OTP. The proposed methodology in [8] provides more control over data stored in system by restricting the access to specific user for specific file with limited privileges and for limited time period on the basis of secret key authentication using symmetric as well as asymmetric mechanism. The integrity and confidentiality of data is fully guaranteed by not only encrypting the data using secret key but also to the access permission and limited file information. Especially, the purpose of the one-time password is to make it more difficult to gain unauthorized access to restricted resources. To overcome these drawbacks, the AES 256 algorithm will be introduced after our one-time password authentication protocol. Thus the proposed system is more secured and can be provide effective authentication.

Paper “Effective Authentication for Avoiding Unauthorized User Access”, presented a modified Role Based Access Control model by extending traditional role based access control in SQL (Structure Query Language) data storage. The said model evaluates and executes security policies which contain versatile access conditions against the dynamic nature of data. The goal of [9] is to devise a mechanism for a forward looking, assertive yet flexible security features to regulate access to data in the data storage that is devoid of rigid structures and consistency. This is achieved by integrating roles and authenticated fine-grained access rules and implemented through effective audit trail. The model and the rules used are presented and show that when implemented, it is capable of outperforming existing models that are role based.

Paper [10] presented a state of art about biometric hand, different techniques used. Biometric is essentially used to avoid risks of password easy to find or Stoll; with as slogan save Time and Attendance. BIOMETRICS is the measurement of biological data. The term biometrics is commonly used today to refer to the authentication of a person by analyzing physical characteristics, such as fingerprints, or behavioral characteristics, such as signatures. Since many physical and behavioral characteristics are unique to an individual, biometrics provides a more reliable system of authentication than ID cards, keys, passwords, or other traditional systems. The word biometrics comes from two Greek words and means life measure. To provide a comprehensive survey, we not only categorize existing biometric techniques but also present detailed of representative methods within each category. Biometrics is a rapidly evolving technology which is being widely used in forensics such as criminal identification and prison security, and has the potential to be used in a large range of civilian application areas. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. It can be used during transactions conducted via telephone and internet (electronic commerce and electronic banking). In automobiles, biometrics can replace keys with key-less entry devices. Although many technologies fit in the biometric space, each works

a bit differently. Relatively new on the biometric scene, face recognition devices use PC-attached cameras to record facial geometry. Once the biometric data is collected, it is encrypted and stored--locally, in the case of the desktop-only products; in a central database for the network solutions. When a user tries to log on, the software compares the incoming biometric data against the stored data.

III. PROPOSED SYSTEM

A face recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. Features like face recognition and One-Time Password (OTP) are used for the enhancement of security of accounts and privacy of users. Face recognition technology helps the machine to identify each and every user uniquely. Fig 1 illustrates the system architecture of proposed system. It consists of a three-step secure authentication process for working employees in their respective organizations.

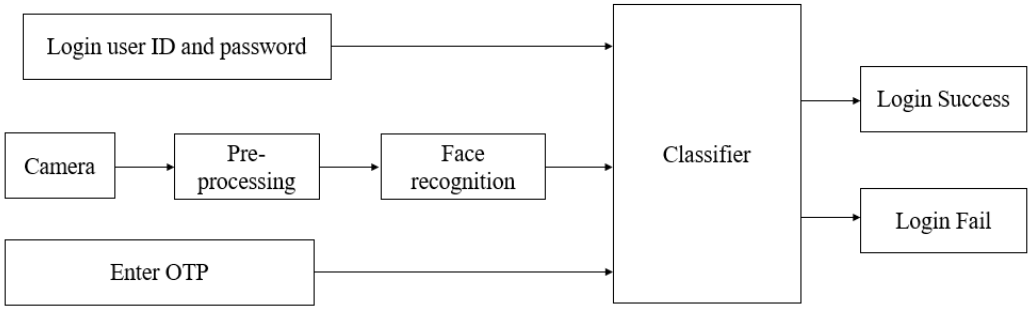

Fig 1: System Architecture of Proposed System

As stated above, at first the user needs to enter the unique login Id and password combination provided to them by the company. Once that matches with the database, next step is to generate the OTP on the registered mobile number. If not, further access to login into the system will be denied. If correct generated OTP is entered into the system, the user moves second step ahead to gain access to the system. Once this is done, next comes the face recognition. With the help of webcams present with each and every system, the face in front of cam is detected. A live image is captured automatically through a webcam installed on the device, which is compared with the image stored in the database. If this image matches, user can get the access to operate that particular system. Haar Cascade Classifier is used to implement face recognition. An additional feature of autosave and auto-logout is also included in this system. Suppose the employee happens to leave their desk due to some reasons, the webcam will be continuously detecting and capturing the images if any. Incase an unknown face image other than that system user, is captured by the webcam, the whole work/data will be automatically saved to the company's server and the system will automatically logout, so that, the unknown user cannot make any manipulations in the users work. The autosave feature helps the user to re-continue the work form the point he/she had left it. Hence a very efficient, safe and reliable system is developed.

IV. CONCLUSION

There has been a use of three tier architecture for providing the authentication and security to the system. Those tiers are login credentials, face recognition and OTP. All these tiers give a great strength for not only providing the authentication but also secure the data in the system. The proposed approach provides more control over the data that stored in the system and restricting the access to specific user for specific file with less privilege and for less time period on the basis of secret key using symmetric as well as asymmetric mechanism. The integrity and confidentiality of data is guaranteed twice by providing encrypting using secret key but also to the access permission and limited file information. Especially, the purpose of the one-time password is to make it more difficult to get illegal access to restricted resources.

- In order to overcome the drawbacks of proposed system if anyone tries to hack the data, the authorized user will get a notification and through an email or message and the authorized user can crash the hard disk. In order to recover it back through particular system software might be needed.
- There can also be changes in the phases of the tool and use anything else as per the convenience of the user. Our system will be compatible with many other types of scanners as well as sensors.
- The same system can be developed in such a way that it can run on multiple operating systems. For now the system used is windows, later it can even be made compatible with mac as well as Linux for user's convenience.

REFERENCES

[1] Patil, A., Rana, D., Vichare, S., & Raut, C. (2018). Effective Authentication for Restricing Unauthorized User. 2018 International Conference on Smart City and Emerging Technology (ICSCET). doi:10.1109/icscet.2018.8537323

[2] IEEE INTERNET OF THINGS JOURNAL 1 Sensor-based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey Mohammed Abuhamad, Ahmed Abusnaina, DaeHun Nyang, and David Mohaisen arXiv:2001.08578v2 [cs.CR] 10 May 2020

[3] A Multimodal Biometric User Verification System with Identical Twin using SVM 2 B.Lakshmi priya, M.Pushpa Rani International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-6, March 2020

[4] Multi-Biometric Authentication Using Deep Learning Classifier for Securing of Healthcare Data Dr. Gandhimathi Amirthalingam1 , Harrin Thangavel Volume 8, No.4, July – August 2019 International Journal of Advanced Trends in Computer Science and Engineering

[5] Cloud security: to prevent unauthorized access using an efficient key management authentication algorithm S. Naveen Kumar1*, K. Nirmala2 International Journal of Engineering & Technology, 7 (1.1) (2018) 607-611 International Journal of Engineering & Technology

[6] On keystrokes as Continuous User Biometric Authentication Suhail Javed Quraishi, Sarabjeet Singh Bedi International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-6, August 2019

[7] A Robust e-Invigilation System Employing Multimodal Biometric Authentication Salam S. Ketab, Nathan L. Clarke, and Paul S. Dowland International Journal of Information and Education Technology, Vol. 7, No. 11, November 2017

[8] EFFECTIVE AUTHENTICATION FOR AVOIDING UNAUTHORIZED USER ACCESS Ms. Chaitali A.Raut International Journal of Recent Trends in Engineering & Research (IJRTER) Volume 04, Issue 07; July - 2018 [ISSN: 2455-1457]

[9] INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 7, ISSUE 11, NOVEMBER 2018 ISSN 2277-8616 182 IJSTR©2018 www.ijstr.org Modified Role Based Access Control Model For Data Security Bukohwo Michael Esiefarienrhe, Abubakar Hashimu Ekka

[10] A SECURITY BY BIOMETRIC AUTHENTICATION Gurudatt Kulkarni1 , Ruchira Chandorkar2 , Nikita Chavan International Journal of Computer Science and Engineering Research and Development (IJCSERD), ISSN 2248- 9363 (Print), ISSN 2248-9371 (Online) Volume 2, Number 1, July-December (2012)