International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 6 ǁ 2022 ǁ PP. 1825-1829

Night Owl- Unauthorized Access Monitoring System

Abhishek K Haris[1], Arathi Anil[2], Athira K R[3], Hrithik Das M[4], Rajesh K S[5]

Department of MCA ,Saintgits College of Engineering (Autonomous) , Kottayam , Kerala, India
[1]PG Student, Department of Computer Applications –Saintgits College of Engineering (Autonomous)
Pathamuttom Kottayam Kerala, India,
[2]PG Student, Department of Computer Applications –Saintgits College of Engineering (Autonomous)
Pathamuttom Kottayam Kerala, India,
[3]PG Student, Department of Computer Applications –Saintgits College of Engineering (Autonomous)
Pathamuttom Kottayam Kerala, India,
[4]PG Student, Department of Computer Applications –Saintgits College of Engineering (Autonomous)
Pathamuttom Kottayam Kerala, India,
[5]Assistant Professor, Department of Computer Applications –Saintgits College of Engineering(Autonomous)
Pathamuttom Kottayam Kerala, India,

ABSTRACT
The unauthorized access monitoring system is Python based desktop GUI developed through Python IDE which allows device admin or company to track, monitor and view system activity. This surveillance enables the system team or authorized personnel to track, record and diffuseunauthorized activity/ malpractice. Through this work, we monitor the system activity of each login.The user will be tracked after logging in, but will not be informed that his/her activity is being tracked. Allactivities performed by the user through the system will be tracked until the hidden process is terminated. The process will be initiated along with the start-up process, during boot time. The system is not supposed to be a breach in privacy of an individual but instead its purpose is intended to allow organizations, system teams and admin to monitor and prevent any unauthorized activity through their system networks.

Keywords: *Unauthorized access, Security, image capturing, keystrokes, geolocation*

Date of Submission: 15-06-2022 Date of acceptance: 30-06-2022

I. INTRODUCTION

Today almost all organizations like colleges, offices andbusiness firms have deployed a large number of computer systems for their day-to-day activities. This can range from study-based application to business needs. All these devices are connected through a network which means that an attack on one system will have repercussions on the entire network. Therefore, it is important that every single system be monitored to protect the network from any unauthorized activity. A vulnerability on any one system within the network can jeopardize the functioning of the organization. It might even lead to data and financial loss. So, there is a need for computer activity monitoring and tracking systems. It ensures that in the absence of the actual user, all the activities taking place within the system are recorded and stored for reviewing purpose. At times, unauthorized users use the system for mal activities by using users login credentials this will put the user in a difficult position. So, we need a system to monitor unauthorized users activities in the absence of the authorized user and tracks these activities. An ideal system monitoring system should have the properties like internet browser history tracking, capturing the image of the unauthorized user, geo location tracking, key strokes tracking..etc. Security and privacy is became one of the major concerns of this time. Security has more important to peoples that are part of a organization. The main objective of this paper is to develop a system that will improve the security of systems that used in organizations. Most of the systems in these organizations are single user systems. So, anyone logged in with the login credentials of actual user and done any mal activities with that system this will put the actual user in a very bad situation. In larger extent there is a chance that this can affect the whole organization. So, a system activities monitoring system would yield great benefits. This will help the users to know about the activities that taken place on the system in the absence of him. also, by using the system that we were developed the user can identify the person who used the system in the absence of him. This can create a large impact. The main aim of our system is to monitor the activities like all browser histories, user's geolocation, keystrokes, and the image of the user.

II. LITERATURE SURVEY

For the development of this work, a review of two research papers was done. In [1], main concern is to train the system in such a way that model first opts to click a pic of user for training purpose, so generally try to click a picture using different facial expressions so that it could address user more easily. And after that, it will train itself with a pic of user and recognize every time when user open web cam. However the big deal is to recognize others as intruders or unknown persons from the known ones i.e., from those whose images were added in the dataset, unless the user introduce others to the web cam.

In [2], it is developed to overcome the difficulties in supervising the student activities in computer laboratories. The implementation of depicted idea helps to prevent malpractice during lab exams using browser, applications/software, pendrive's and maintain the discipline during student's practical performance. In this work, Raspberry pi is used as a centralized network Server and socket programming is used to provide communication between computers and centralized network server. Keyboard and mouse theft protection is also provided for safeguarding lab belongings. The fire alarm system is an add-on to detect the presence of smoke inside the lab in case of any fire accident. Additionally, RFID based data logging system is used to store a data in an excel sheet for the time-in and time-out of students during the lab conduction. This work also emphasizes on surveillance of computer labs with the help of camera. The overall programming is developed using python and java. The system is capable of notifying the lab in-charge through E-mail with snaps attached to it and also through buzzer and LED light indication in case of any event or issues.

The system which is proposed by us protection is done by monitoring the system and storing unauthorized users activities within the system. The unauthorized access monitoring system will help the users to understand whether there any mal-activities taken place in system in the absence of actual user. User image capturing and tracking of keystrokes, browsing history and geolocation identification will make the system more secure.

III. METHODOLOGY

Monitoring of system activity is done by creating a process. Here we are aiming to monitor system activities on each login, once process is activated by user. Then the specified activities will be tracked and stored withing the system until the hidden process is terminated.

The process will be hidden. Admin have to activate the process. The process will be initiated along with the start-up process, during boot time. The keystrokes are tracked to identify the activities performed on the keyboard.User image capturing used to capture the high-resolution, high-quality photos and autofocus functionality, Browsing History is tracked to record the web histories and Geolocation identification is used to identify the geographic location of a user or computer system via a variety of data collection mechanisms are the user activities used in the system. System will be more secure and easy to use.

3.1 ALGORITHM

The biggest dilemma is to decide which algorithmsshould we use to train the pictures and let our computers or machines recognize the people all by its own. All of these come under the classification algorithm in supervised learning where we create labels according to the same types of data input so that computer can easily recognize peoples or anything for which it is train. The first basic thing we should do is to create an empty list of labels to gives labels to each and every image of different objects so that we could easily store them. But how does it start from the beginning. Actually, here we are giving the inputs of data which is in the form of images. For taking images from the web camera of the laptop, the very basic thing one should do is to import cv2 which helps to read and display a video stream. And after reading the image from the web camera, we have to give labels to the image with which we are going to train our machine or our computer so that they recognize it more easily. After that, web camera captures the image in different angles so that in any angle it can recognize the image and tells the name as given in the label. Here, we have trained our computer to take up to 50 pictures of image in different angles. The user can add as many images he/she wants. Adding many images will increase the accuracy of the work. After adding many images or a single image, user can now train the system. Adding images to train our computer or machine is an easy task. We just have to use cv2 library which helps one to access the web camera so that one could read the image. Adding labels to an image is like adding name to an image. Like we do in supervised learning, we give labels to the input where first computer observes all the input by taking some time and then learns from the input and then able to predict the real time things. Just like we do it to train with only 50 pictures per image. Anyone can use more than 50 pictures or less than 50 pictures to train a model. It all depends on the user choice who wants to train a model. After taking pictures the next thing is to train the model by one of the classification algorithm in machine learning. This is the biggest deal any user will face as the best part is to select which algorithm one should choose while using in a model, which will give best result or perfect result which accuracy will be the best, which result will match the result in the future if one is solving real time problem like stock prediction. All things should keep in one‘s mind before using the algorithm.

Step 1. Make our own dataset by capturing images in real time where we have put a limit on the number of images to be captured by the system is 50.

Step 2. Give label to the dataset here we consider label as name.

Step3.Usingknn (k nearest neighbor) of supervised learning where computer is trained to learn from the dataset, so after adding label and capturing images i.e., making our own dataset we have to train our model.

Step 4. After training the data through supervised learning, 80% of the data which is present in the dataset is used to train while remaining 20% of the data is used to test

Step 5. After training we will use it for testing whether it is able to recognize the persons.

Step 6. When used for testing purpose, it is used to recognize only those persons whose label i.e., name is added while for rest of the persons, system claims them as an intruder.

3.2 SCREENSHOTS AND FIGURES

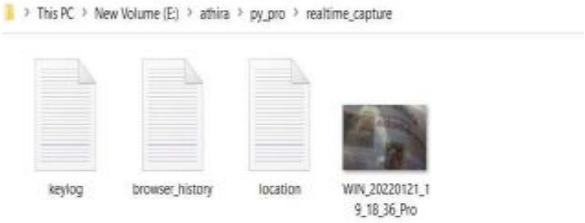
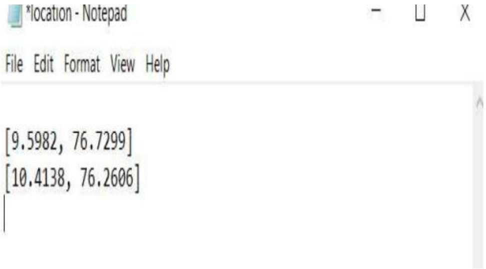
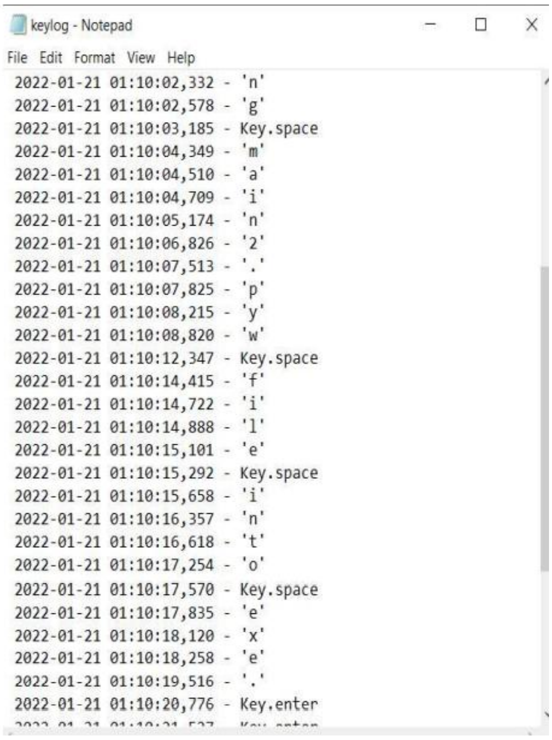

This PC > New Volume (E:) > athira > py_pro > realtime_capture
keylog
browser_history
location
WIN_20220121_19_18_36_Pro

Fig. 1 stored folder



```
[9.5982, 76.7299]
[10.4138, 76.2606]
```

Fig. 2 location coordinates



```
2022-01-21 01:10:02,332 - 'n'
2022-01-21 01:10:02,578 - 'g'
2022-01-21 01:10:03,185 - Key.space
2022-01-21 01:10:04,349 - 'm'
2022-01-21 01:10:04,510 - 'a'
2022-01-21 01:10:04,709 - 'i'
2022-01-21 01:10:05,174 - 'n'
2022-01-21 01:10:06,826 - '2'
2022-01-21 01:10:07,513 - '.'
2022-01-21 01:10:07,825 - 'p'
2022-01-21 01:10:08,215 - 'y'
2022-01-21 01:10:08,820 - 'w'
2022-01-21 01:10:12,347 - Key.space
2022-01-21 01:10:14,415 - 'f'
2022-01-21 01:10:14,722 - 'i'
2022-01-21 01:10:14,888 - 'l'
2022-01-21 01:10:15,101 - 'e'
2022-01-21 01:10:15,292 - Key.space
2022-01-21 01:10:15,658 - 'i'
2022-01-21 01:10:16,357 - 'n'
2022-01-21 01:10:16,618 - 't'
2022-01-21 01:10:17,254 - 'o'
2022-01-21 01:10:17,570 - Key.space
2022-01-21 01:10:17,835 - 'e'
2022-01-21 01:10:18,120 - 'x'
2022-01-21 01:10:18,258 - 'e'
2022-01-21 01:10:19,516 - '.'
2022-01-21 01:10:20,776 - Key.enter
```

Fig. 3 key capturing

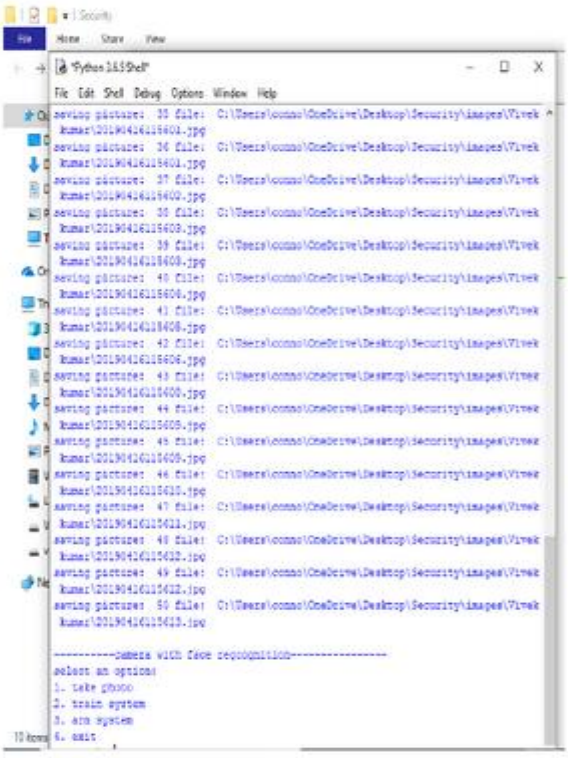
IV. EXPERIMENT AND RESULTS

This model always asks the user whether he/she have to take a pic or not, whether he/she have to train the image or whether he/she wants to check whether a computer can recognize or not.

This system is trained to capture a picture of 50 images. One can increase the no of pictures taken by the system. It all depends on the user‗s choice. We are interested only in taking 50 pictures because this is a prototype.

After taking or capturing images, the next thing one should do is to train the image. Just like supervised learning do after observing the inputs, it trains itself in the same way after capturing the images computer or machine will train itself from the past data. Here, past data is the images. Computer will train itself to each and every image of a label. Machine learning generally trains data either on 80-20 or 70-30. This means that up to 80% of full data is used for training purpose and the rest 20% is used for testing purpose or 70% of the full data is used for training purpose and rest 30% is used for testing. After training the next thing is to check how much a computer trains itself, through observing and training. Here, we will check whether our system or computer is able to recognize itself or not. If it is able to recognize the path, then our model is successful. In this we have to set a path to the trained model, so that computer able to recognize each and every object which is trained.

And this model is made to recognize a certain group of people, if another person comes in contact with the known person by the computer then computer name that person as an intruder. After capturing the images and training the images, the next thing a user wants to see whether a computer is able to recognize a person or not. The next thing to test is to whether can recognize the unknown persons or not. We have trained ―intruder‖ word to those whom computer or system becomes unable to recognize. In this model, computer is trained only to recognize a single person. This model is trained to recognize and detection of face only, one can use it to recognize face and eye both.



```
saving picture:  35 file:  C:\Users\conno\OneDrive\Desktop\Security\images\Vivek
 kumar\20190426115601.jpg
saving picture:  36 file:  C:\Users\conno\OneDrive\Desktop\Security\images\Vivek
 kumar\20190426115601.jpg
saving picture:  37 file:  C:\Users\conno\OneDrive\Desktop\Security\images\Vivek
 kumar\20190426115602.jpg
saving picture:  38 file:  C:\Users\conno\OneDrive\Desktop\Security\images\Vivek
 kumar\20190426115603.jpg
saving picture:  39 file:  C:\Users\conno\OneDrive\Desktop\Security\images\Vivek
 kumar\20190426115603.jpg
saving picture:  40 file:  C:\Users\conno\OneDrive\Desktop\Security\images\Vivek
 kumar\20190426115604.jpg
saving picture:  41 file:  C:\Users\conno\OneDrive\Desktop\Security\images\Vivek
 kumar\20190426115605.jpg
saving picture:  42 file:  C:\Users\conno\OneDrive\Desktop\Security\images\Vivek
 kumar\20190426115606.jpg
saving picture:  43 file:  C:\Users\conno\OneDrive\Desktop\Security\images\Vivek
 kumar\20190426115608.jpg
saving picture:  44 file:  C:\Users\conno\OneDrive\Desktop\Security\images\Vivek
 kumar\20190426115608.jpg
saving picture:  45 file:  C:\Users\conno\OneDrive\Desktop\Security\images\Vivek
 kumar\20190426115609.jpg
saving picture:  46 file:  C:\Users\conno\OneDrive\Desktop\Security\images\Vivek
 kumar\20190426115610.jpg
saving picture:  47 file:  C:\Users\conno\OneDrive\Desktop\Security\images\Vivek
 kumar\20190426115611.jpg
saving picture:  48 file:  C:\Users\conno\OneDrive\Desktop\Security\images\Vivek
 kumar\20190426115612.jpg
saving picture:  49 file:  C:\Users\conno\OneDrive\Desktop\Security\images\Vivek
 kumar\20190426115612.jpg
saving picture:  50 file:  C:\Users\conno\OneDrive\Desktop\Security\images\Vivek
 kumar\20190426115613.jpg

----------camera with face recognition---------------
select an option:
1. take photo
2. train system
3. arm system
4. exit
```

Fig.4: System is capturing the images

The unauthorized access monitoring system will help the users to understand whether there any mal-activities taken place in system in the absence of actual user. User image capturing and tracking of keystrokes, browsing history and geolocation identification will make the system more secure.

V. CONCLUSION AND FUTURE SCOPE

The paper entitled 'Night Owl" is completed on time and found working effectively under the circumstances that arrives in the real environment using the facilities and functionalities of Python and Open CV. The system is user friendly and is well to make easy interaction with the user of the system. The speed and accuracy are maintained in a proper way. Testing of the system has given good result. The processing of the system is simple and is in regular order. We believe that all the object is of the required system are met in the system. It is done with an insight into necessary modifications that may be required in the future.

To survive from the competition each system has to produce some modifications in the future. New features will be provide the system a new fresh look, by which it can attract a lot of users. Due to this reason it's necessary that the system need to be modified. This paper is effective and easy to use. All modules satisfy user needs perfectly. This system could solve the problem faced by the existing system by including a number of features, which help in reducing the complexity and difficulties. The system ensures reliability, accuracy, security, and user friendly. It makes sure that the users get maximum advantages and the administrator can work more effectively.

However this is a prototype for this system, but if we able to build the real model using night vision camera, human presence sensor to reduce power consumption, this will be the best thing for the security of our county‘s confidential things.

REFERENCES

[1]. SaikatMaity,Vivek Kumar Jha,Overcoming Security issues using OpenCV and Machine learning, INTERNATIONAL JOURNAL OF COMPUTER TRENDS AND TECHNOLOGY (IJCTT) – VOLUME 67 ISSUE 5- MAY 2019 Ali. J. and Dyo, V. (2020) "Practical Hash-based Anonymity for MAC Addresses". The 17th International Conference on Security and Cryptography

[2]. Deepa N P, Mahesha P, Nagendra K N, Madhu G Amalazari, Sunil Kumar T, Detection And Monitoring Of Unauthorized Use Of Computers In The Computer Laboratory, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 8, ISSUE 09, SEPTEMBER 2019

[3]. M.H.A. Wahab et al., "Web-Based Laboratory Equipment Monitoring System Using RFID," 2010 International Conference on Intelligent and Advanced Systems, Manila, pp. 1-5, 2010. DOI: 10.1109/ICIAS.2010.5716177

[4]. E. T. Kitova, N. I. Gorlov and I. V. Bogachkov, "Unauthorized Access Monitoring in Optical Access Networks," 2020 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), 2020, pp. 1-4, doi: 10.1109/SYNCHROINFO49631.2020.9166039.

[5]. J. Shi, R. Li and W. Hou, "A Mechanism to Resolve the Unauthorized Access Vulnerability Caused by Permission Delegation in Blockchain-Based Access Control," in IEEE Access, vol. 8, pp. 156027-156042, 2020, doi: 10.1109/ACCESS.2020.3018783.

[6]. G. Teng, Y. -w. Ding and S. -c. Dai, "Research of Access Control of USB Storage Device with Information Security in Unauthorized Internet Access Monitoring System," 2009 International Conference on Computational Intelligence and Software Engineering, 2009, pp. 1-5, doi: 10.1109/CISE.2009.5366671.

[7]. T. V. Ortiz, B. Y. L. Kimura and V. Rosset, "Unauthorized access based on HTTP redirection and MitM — UARiM," 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), 2017, pp. 1-6, doi: 10.23919/CISTI.2017.7975954.

[8]. Robert N. Reid, "Chapter 10 Intrusion Detection Preventing Unauthorized Access," in Facility Manager's Guide to Security Protecting Your Assets , River Publishers, 2005, pp.165-182.

[9]. Y. Li, Y. Yang, X. Yu, T. Yang, L. Dong and W. Wang, "IoT-APIScanner: Detecting API Unauthorized Access Vulnerabilities of IoT Platform," 2020 29th International Conference on Computer Communications and Networks (ICCCN), 2020, pp. 1-5, doi: 10.1109/ICCCN49398.2020.9209626.

[10]. M. Habiba, M. R. Islam and A. B. M. S. Ali, "Access Control Management for Cloud," 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013, pp. 485-492, doi: 10.1109/TrustCom.2013.61.