International journal of advances in engineering and management (IJAEM)
Volume 3, issue 6 June 2021, pp: 1957-1964 www.ijaem.net ISSN: 2395-5252

Intelligent Intrusive Detection System

Chaitanya Sagar, Durga Puri, Swati, Sidharth Dhamija, Mr. Jogendra Kumar
Department of Information Technology Dr.Akhilesh Das Gupta Institute of Technology and Management, New Delhi(India).
Department of Information Technology Dr.Akhilesh Das Gupta Institute of Technology and Management, New Delhi(India)
Department of Information Technology Dr.Akhilesh Das Gupta Institute of Technology and Management, New Delhi(India)
Department of Information Technology Dr.Akhilesh Das Gupta Institute of Technology and Management, New Delhi(India)
Mentor, Department of Information Technology Dr.Akhilesh Das Gupta Institute of Technology and Management,
New Delhi(India)

Submitted: 05-06-2021 Revised: 18-06-2021 Accepted: 20-06-2021

ABSTRACT - Physical surveillance is entirely dependent on humans and closed-circuit cameras. Various recent instances have proven that current scheme of surveillance is not effective. Hence, there is a need of a system that could automate entire surveillance and detect any intrusion. Intelligent Intrusion Detection System (IIDS) is a system to detect physical intrusion in a premise. System uses advanced Computer Vision techniques along with Machine Learning algorithms to make decisions. Systems uses face detection scheme to identify intruders, uses different encryption schemes to maintain data security and privacy.

I INTRODUCTION

Rate of crime against enterprises and personal computing spaces is increasing at an alarming rate. It can be either physical or digital in nature. Digital crimes are prevented to a large extent by sophisticated software that prevents attacker from doing any unwanted act. Whereas to prevent physical crimes, enterprises are still largely dependent on human surveillance and monitoring. Intelligent Intrusion Detection System (IIDS) uses computer vision and artificial intelligence techniques to monitor each and every movement and also detect suspicious movements within time so that necessary actions are taken.

IIDS is trained before deployment to recognize people. It detects each and activity and informs its administrator through various methods about the suspicious activities. It also keeps a record of every separately in the server done by recognized and unrecognized person. This record can be used as a digital evidence in future.

Modern day security systems don't offer high security, they are basically footage saving systems that record the footage of the scene and don't raise any alert messages even if there is a threat or actual crime occurring. Authors have developed a system that not only captures the footage but also detects any suspicious activity. This was made possible by adding computer vision and neural network modules that will process the live feed of the camera look for any possible threats and raise a security alert message so that necessary action can be taken while the activity is being performed.

System uses machine learning algorithms to recognize faces and making decisions on whether person is an intruder or a trusted employee of the organization. Other features of system include advanced asymmetric encryption schemes for data prevention, email alert system for informing system administrator about significant activities, logging mechanism to store information which may later be used as evidence in case of any unfortunate incidents. Authors have also proposed extra features for further releases of system, including sentiment analysis of intruder's voice sample and speech to text translation of intruder's voice.

II PROJECT FEATURES AND OPERATION

II.A WatchDog System

WatchDog is one of the core features of IIDS, it is responsible for the security of the software, it makes sure that no one messes around with important files of the IIDS system, if it finds out that an attempt to modify or delete the IIDS files has been done then it send the admin an alert message regarding this issue and it automatically corrects the files , if anyone tries to delete the file then this module will automatically

International journal of advances in engineering and management (IJAEM)
Volume 3, issue 6 June 2021, pp: 1957-1964 www.ijaem.net ISSN: 2395-5252

paste the correct copy of the file that needs to be there, Watchdog is basically a temporary program that IIDS generates every time when the IIDS system is shut down . After the system is turned off the program takes control of the files and makes sure that they remain safe, when the IIDS system is turned on it kills the watchdog program running in the background and destroys the old watchdog program files, as the IIDS system will not be affected in any way if these files are deleted when the system is on because the system will create those files anyway before shutting down, these IIDS files are just needed to provide data to the system in order to initialize.

IIDS system stores the important files in the APPDATA directory of windows if anyone manages to reach that directory and delete those files then the invisible instance of watchdog will automatically add the removed files , the watchdog instance cannot be traced in the task manager window as it runs in the background using VB Script which makes it hidden and it given a different Name when it is operating so that it cannot be traced using task finding commands , only IIDS core has the method to destroy the instance hence ensuring high security. Watchdog broadly has 2 tasks, first look for the presence of the important files and check the content of the important files, if any of the check fails then it performs the needed action

To find out whether someone tried to delete the files IIDS system check the content of the file as the watchdog system adds secret string in the end of the file which isn't visible through the text editor, when the IIDS core finds that extra added value then it removes it and generates a high alert mail and sends it to the admin.

II.B IIDS UI and Operations

The first screen that is visible after the user initializes the app is Login Screen after adding the credentials and performing a successful login user gets access to the Admin Panel which provides the user 3 main controls , first is to check the live stream that IIDS is scanning, second is to check the Logs which IIDS is generating after analyzing the video stream and third is add member control which allows the user to add pictures of the objects or person that the user wants the system to recognise as employee/object to be taken care of. The whole UI system is a tree structure, Top is the main window node which displays everything and all the other elements that are visible in the window are children of this node in some cases a UI node can further have UI node as a child, as the user accesses different features of IIDS these nodes are added and removed accordingly, fir example when the IIDS is initialized the first screen has a TOP node with User ID text UI node and User ID entry field UI as children along with other UI elements when the user logs in successfully the system destroys all the nodes mentioned above and creates 4 Button UI nodes which user authority to access the 3 features and shutdown system.

The tree system makes it easy to manage the layout of the app without making thing much complicated and also reduces the memory overhead which might be created if the elements nodes are just hidden instead of deleting them, memory overhead can slow down system so this method helps in keeping the IIDS performance pretty stable. Memory overhead elimination comes at the cost of slightly increased time due to repeated allocation and deallocation of memory for the UI nodes but the time increase is so less that it isn't noticeable

UI elements present in the first page:

- 3 Text UI nodes
- 2 Text field UI nodes
- 1 button UI node

Fig 3.1 Fill the required details

UI elements present in welcome page(visible only first time when user has to enter the login detail and email ID to login nextime)

- 4 text UI nodes
- 3 text field UI nodes
- 1 button UI node

International journal of advances in engineering and management (IJAEM)
Volume 3, issue 6 June 2021, pp: 1957-1964 www.ijaem.net ISSN: 2395-5252

Fig 3.2 Restart the access panel after updation of details

After the user enters the login credentials for the first time the user is redirected to restart page in which the user get a message that the user data is saved and for the new login credentials to take effect the user has to restart the app this page has

- 1 text UI node
- 1 button UI node

Fig 3.3 In access area

After restarting the app the user needs to enter the new login credentials else an error message will be displayed the error message panel consist of following elements

- Panel UI node
- Message UI node
- Button UI node

Fig 3.4 Logged Out

The message UI node and button UI node are children of Panel node.
If the user enters the correct login credentials the user directed to Admin control panel, this panel has the following UI nodes

- 1 text UI node
- 4 button UI nodes

International journal of advances in engineering and management (IJAEM)
Volume 3, issue 6 June 2021, pp: 1957-1964 www.ijaem.net ISSN: 2395-5252

Fig 3.5 In access area

The four button help user in operating the system, the button are:

- Watch Live stream button, this open up the live stream that is being captured by the IIDS system if the debugger mode is on the sub stages of Live stream analysis are also get shown

Fig 3.6 Live Feed

- View logs button this opens up a panel with the logs that are being generated by the IIDS system

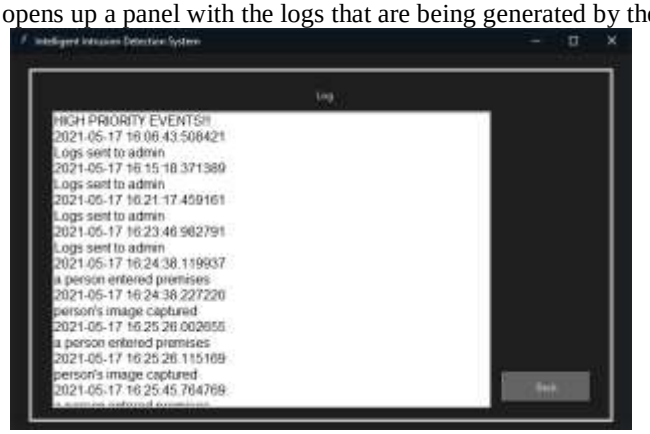

Fig 3.7 Log

- Add Member button, this helps the user to take 100 pictures of the employee or object that user wants IIDS to keep a track of, after taking 100 pictures the system automatically starts training itself so that IIDS core starts identifying that particular object or person

International journal of advances in engineering and management (IJAEM)
Volume 3, issue 6 June 2021, pp: 1957-1964 www.ijaem.net ISSN: 2395-5252

I ENCRYPTION SCHEME

There are three different encryption schemes used at different levels of project. Encryption was required in order to hide important confidential data like the User Name, Password, User Email ID and activity logs. Different encryption algorithms are described below:

III.A ASCIIMax Encryption Scheme :

In this encryption scheme the string that has to be encrypted is taken and ASCII value of each character in the string is compared in order to obtain maximum ASCII value. Then all the characters are converted into their respective ASCII codes these ASCII codes are later divided by the maximum ASCII value obtained in the previous stage, the list of floats so generated constitute the part of encrypted message the value of these floats is in the range of 0 to 1 , now to decrypt this text the maximum ASCII value is needed this value is hidden in the form of float value along with the float list that was generated by previous process, here's an example of how the maximum ASCII value is hidden in the form of float value.

Let's say that maximum ASCII value is 220 then to hide this value some random value is added to this ASCII value say, 650 now the new value is 870, to make it look like other float values a random float value is concatenated before this value which is generated by random function, let's say that the random function generated a value "0.897" the final value will be "0.897870" , while decrypting the decrypter will remove the extra value added by random function and them subtract 650 form the value obtained to get the maximum ASCII value which is 22 in this case and then to obtain the string all floats will be multiplied by this ASCII value to obtain the ASCII values of all the characters in the string and finally these ASCII values will be converted to corresponding characters. Since this is a new encryption scheme the attacker will have no idea about what do the float values means and even if the attacker figures out the scheme it will be hard to find out the float value which has the hidden ASCII value and cracking the ASCII value from the float value is also not easy as it has a random number added to it and an random float number concatenated to itself.

Fig 3.8 ASCIIMax Encryption

III.B Login Credentials Encryption:

To encrypt the login credentials passlib library was used , it helps in generating hashes , the user ID and password were repeated hashed for 20 million times and a salt was also added to make hacking of the user credentials difficult, to login the user enters the Login credentials which are then compared to the hash values generated initially , passlib provides a provision just to compare the two values and does not convert the hash back to user credential to compare the entered value, this is done in order to avoid leaving any kind of trace which can be used a security breach point, the hashing method used is SHA256, it generates 256 bit hashes which more difficult to crack and on top of that he the high iteration count makes it nearly impossible for the attacker to break the code and gain access of the system.

III.C ETBE Scheme :

ETBE scheme stands for Extended Text Base64 Encryption scheme. This encryption scheme is followed to encrypt the system logs. It is an asymmetric encryption scheme i.e. it encrypts the same text and gives a different cipher text for it. The major advantage with this encryption scheme is that it becomes extremely difficult for any attacker to reverse encryption scheme and understand the actual message if it is not intended for that user. Encryption scheme adds two random character strings both at the beginning and ending of actual string in to increase string's length and then encrypts it using open ssl base64 encryption. This way it becomes extremely difficult to break encryption scheme and understand the actual mechanism. This scheme is used to encrypt all system logs stored. This step increases the data security and its privacy making system even more reliable.

International journal of advances in engineering and management (IJAEM)
Volume 3, issue 6 June 2021, pp: 1957-1964 www.ijaem.net ISSN: 2395-5252

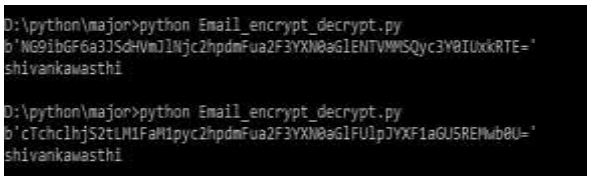

Fig 3.9 ETBE Scheme

IV EMAIL INFORMATION SYSTEM

Project uses email as medium for sending system related information. It sends all the necessary information to keep the system administrator posted about the working of system. The system sends information through email in three conditions:

- First condition is when an intruder enters the area of surveillance, system decides on the basis of its learning if the person is an intruder or a trusted personnel. In case of a trusted personnel information is logged for future usage and in case the person is identified as an intruder then system generates an email mentioning that an intruder entered premises and it also attaches the image of that intruder for purpose of evidence and necessary course of action.
- Second condition is when system is closed or shut down, since the nature of system is that of a surveillance system it is never meant to be closed and if goes down or someone tries to shut it down deliberately then system administrator must be informed. In this case email informs system administrator that system went offline and it attaches a snapshot of system logs with the email for evidence and necessary course of action. This entire log is encrypted in asymmetric encryption scheme and is decrypted just before sending the email. Traces of decryption are immediately removed from the system for enhancement of overall system security.
- Third condition is when a malicious user tries to intentionally remove system files. This is one of the high alert situation and it needs immediate supervision so system administrator is informed about the same so that it could be dealt with and in the meanwhile malicious user is not allowed to access that content.

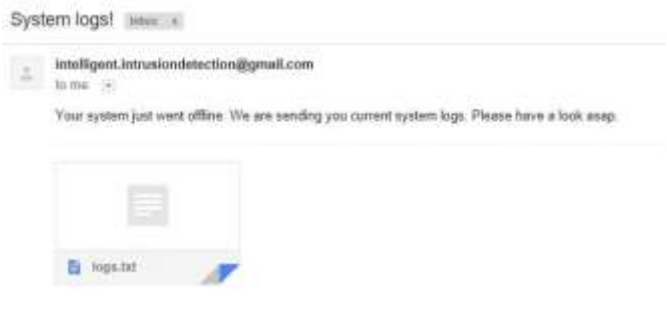

Fig 3.10 Current log mail sent

Fig 3.11 Intrusive Found

International journal of advances in engineering and management (IJAEM)
Volume 3, issue 6 June 2021, pp: 1957-1964 www.ijaem.net ISSN: 2395-5252

Fig 3.12 Activity done by intruder

V LOGGING MODULE

Logging module is another important aspect of system. Every important system activity is logged and saved in the logging module. This module keeps track of a wide range of activities like:

- System boot timestamp, which basically tells the timestamp at which the system was activated.
- Timestamp when intruder was seen in the premises for the first time, it basically is the timestamp when intruder is seen in front of the camera for the very first time.
- Timestamp when intruder's image was captured by the system.
- Information about intruder if his image was captured or not. This is helpful in cases if the image gets deleted accidentally.
- Decision output if the person entering the premises is an intruder or a trusted personnel, this is done on the basis of a machine learning algorithm that can recognise faces.
- Timestamp of the information email if the person is identified as an intruder and if it was sent or not to system administrator.
- Timestamp if the system is closed or shut down.

Logging module uses end to end encryption which is asymmetric in nature to enhance the data security and its privacy. Data stored in the log module uses Sql structure and syntax which provides freedom of cross platform operability. Events in logging module are broadly categorized into:

- High Priority Events
- Low Priority Events

This categorization is done on the basis of events that can or cannot affect system's working. Events like deletion of files can pose a serious threat to system and they need immediate attention so they are placed in high priority events whereas activities like system initialization are not that bigger threat.

VI FACE RECOGNITION MODULE

This is the most critical module of the entire system. This module decides if the person entering the premises is a trusted individual or some malicious intruder. This is achieved by using Computer Vision APIs like TensorFlow. System is trained to recognise faces of people for which it is trained. The entire working mechanism of this algorithm is explained below:

- Training is the first step in the face recognition module. Module is fetched a huge dataset of facial images of target faces which are to be recognised by the system. This dataset serves as the knowledge for the module to understand the faces better.
- On the basis of this training data, system creates a graph of all the values and of the data extracted. This data is then used to further test and then identify image or classify them.
- Testing is the next step after training, in this step it uses the graph obtained from training and uses it to validate certain data and their corresponding labels. System has shown a training efficiency of 92% and testing efficiency of 95%. It was trained for 500 steps of training and testing cycles and over a few thousand of images.

This module judges an image on labels for which model is trained. It predicts a probability score along with the prediction of labels for every image being classified. It then passes the predicted label to the email information module which then proceeds with further steps.

VII RESULTS

IIDS passed all the basic and extreme situation tests, the first test was to see how well it protects the User's details and Log, since IIDS uses various encryption algorithms and many of them are newly created algorithms which are hard to crack it becomes nearly impossible for the attacker to collect any data , the second test was to check the ability to handle attack on core features, and as results show that IIDS was able to to handle any kind of attack on it's core files that it needs in order to operate as there is a background program "WatchDog" that takes care of all the files and just in case any file gets deleted the program creates a new copy of the files and also makes sure to introduce a special character which is used later on to detect an attack attempt, in such a

situation the software also intimates the admin about such activities.

The third test was to see whether the system is able to analyze the feed that it's capturing via webcam, results show that it was able to identify objects in the visible in the viewport and on the basis of activities of the objects it was also able to detect suspicious activities, which is the objective of the project, the system also generates logs on the basis of its analysis of feed and it also keeps intimating the Admin about the logs on regular get basis. The system was also highly adaptive as it easily gets trained to identify new objects and people and does not get fooled by minor changes in the facial features like length of the hair including facial hair.

VIII CONCLUSION

All the decided targets were met in the given time and all the features of this project stand upto the expectations, this project has a very good potential use in any industry that is currently dependent on human surveillance as it can safely replace all the human labour as it over all performance is greater and the cost of operation is really low and the only possible expenditure is maintenance cost. This system can run 24 x 7 without fatigue which is the main cause of failure of human surveillance method. However there is still scope of improvement in this which we plan to add in the upcoming updates of this project. Features that will be added in the future updates are sentiment analysis of the audio stream to find out the intentions of the person and adding compatibility for depth sensors camera and night vision cameras which will improve the performance of this system by many folds.

REFERENCES

[1]. http://www.psych.utoronto.ca
[2]. Y. Choi et. al., "Energy-efficient design of processing element for convolutional neural network," in IEEE Transactions on Circuits and Systems II: Express Briefs, unpublished.
[3]. G. Nápoles et. al., "Fuzzy-Rough Cognitive Networks," in Neural Networks 97 (2018) 19 – 27, http://doi.org/10.10.16/j.neunet.2017.08.007.
[4]. S.B. Maind and P. Wankar, "Research Paper on Basic of Artificial Neural Network," in International Journal on Recent and Innovation trends in Computing and Communication, Vol.2, Issue 1, pp. 96-100, ISSN: 2321-8169.
[5]. K. Arora, S. Suri, D. Arora and V. Pandey, "Gesture Recognition Using Artificial Neural Network," in Intenational Journal of Computer Science and Engineering, Vol. 2, Issue 4, E-ISSN: 2347-2693.
[6]. Z. Zhou and K. Huang, "Research on a Combined Neural Networks Prediction Model for Uran Traffic Volume," in International Seminar on Future Biomedical Information Engineering, DOI: 10.1109/FBIE.2008.15
[7]. S. A. Naseer, I. Zaqout, M. A. Ghosh, R. Atallah and E. Alajrami, "Predicting Student Performance Using Artificial Neural Network: in the Faculty of Engineering and Information Technology," in International Journal of Hybrid Information Technology, Vol. 8, No. 2 (2015), pp. 221-228, http://dx.doi.org/10.14257/ijhit.2015.8.2.20.
[8]. A.E. Shivdas, "Face Recognition using Artificial Neural Network," in International Journal of Research in Management, Science and Technology, Vol. 2, No. 1, April 2014, E-ISSN: 2321-3264.
[9]. Li Xiaodong et.al., "Widely Linear Quaternion Unscented Kalman Filter for Quaternion-Valued Feedforward Neural Network" in IEEE Signal Processing Letters, 2017.
[10]. WolfGang Maass, "Networks of Spiking Neurons: The Third Generation of Neural Network Models", Institute for Theoretical Computer Science, Austria, 2017.
[11]. Abdelhalim Hiassat et. al., "A genetic algorithm approach for location-inventory-routing problem with perishable products" in Journal of Manufacturing Systems, 2016, pp. 93-103.
[12]. Stephen Grossberg, "Nonlinear Neural Networks: Principles, Mechanisms and Architectures", Neural Networks, Vol. 1, pp. 17-61, 1988.
[13]. Xingbao Gao and Li-Zhi Liao, "A Novel Neural Network for Generally Constrained Variational Inequalities" in IEEE Transactions on Neural Networks and Learning Systems, 2016.