IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

ATM FRAUD DETECTION AND ENHANCING SECURITY

Dr K.S. Rajesh
Dept. of AIML
RajaRajeswari College of Engineering
(Affiliated to VTU)
Bangalore, India

Afzal Ulla
Dept. of CSE
RajaRajeswari College of Engineering
(Affiliated to VTU)
Bangalore, India

Aman Aryan
Dept. of CSE
RajaRajeswari College of Engineering
(Affiliated to VTU)
Bangalore, India

Ashish Ashok Naik
Dept. of CSE
RajaRajeswari College of Engineering
(Affiliated to VTU)
Bangalore, India

Bhargav H Praksah
Dept. of CSE
RajaRajeswari College of Engineering
(Affiliated to VTU)
Bangalore, India

Abstract: Quick improvement in science and innovation, advancements are being developed and this has had a constructive outcome generally speaking, however different monetary foundations are as yet exposed to robberies and cheats. ATM terminals are intended to work with more straightforward withdrawal of cash for the clients. ATM lays out the security of the foundation in incredible arrangement as a result of their number of bank exchanges. Because of their accessibility and general ease of use ATMs have become exceptionally well known with overall population. The current system requires the user to insert his card into the ATM where the data of the user is collected through the help of the card and that data is authenticated with the help of the static key called as PIN. This PIN is entered by the user in the user interface of the atm machine. After the PIN gets verified the user can proceed with the further transaction activities. In the current system, anyone who knew the Personal Identification Number can use the card for transactions with or without the account holder's approval. Because the Personal Identification Number is unchanging , thieves can easily gain it from users through hacking the atm machine or muscle strength. In some regions, people are threatened in front of ATMs, and the PIN security feature is useless in these instances. The majority of people utilize an ATM for a variety of reasons and in a variety of situations. The most typical three circumstances are examined, and solutions are discovered. The ATM machine is being used by the user as himself. If the user is intimidated by someone who wants to take money from him or her without his or her consent. If a user's companion uses user card for transaction.

IndexTerms— ATM, Face Recognition, Pattern Matching, Machine Learning, Rest API.

I. INTRODUCTION

ATM gives PIN (Personal Identification Number) to every one of its clients with the assistance of which they can get to their record. To complete shoppers ATM monetary exchanges or potentially banking capacities whenever ATMs are free consistently. Since the exchange is for the most part reliant upon PIN-based check a few ease-of-use factors have been examined to improve the security for confirmation of clients at ATM. The main drawback of this methodology is that once the Personal Identification Number (PIN) is figured out, anyone can be uses it to withdraw amount. Face-id is used as a key to solve this problem. A image (facial) recognition system is a program or instructions that recognizes or confirms a person's face from the digital image data or a video from a video resources. For facial

recognitions, there are two sorts of correlations. The first is confirmation, which is when the framework compares the given individual to who that individual claims to be and provides a yes or no response. The next one is ID, which is where the framework compares the provided individual to a large number of other people in the data collection and generates a ranked list of matches. Face recognition innovation looks at the unique form, appearance, and positioning of face features. Face recognition is a mind-boggling technology that is mostly based on programming. The Biometrics main benefit is that it is unique to each individual. The planned development is unquestionably not a viable alternative for standard ATM security. The proposed improvement is seen as a supplement to the current plan where time consumption of the transaction process is not delayed by the extra face recognition process. The atm should be connected to the database of the user to fetch the user data and authenticate the user inputs and further to go with the transaction. The proposed software increases the efficiency of the ATM's.

II. EXISTING SYSTEM

The current system requires the user to insert his card into the ATM where the data of the user is collected through the help of the card and that data is authenticated with the help of the static key called as PIN. This PIN is entered by the user in the user interface of the atm machine. After the PIN gets verified the user can proceed with the further transaction activities. In the current system, anyone who knew the Personal Identification Number can use the card for transactions with or without the account holder's approval. Because the Personal Identification Number is unchanging, thieves can easily gain it from users through hacking the atm machine or muscle strength. In some regions, people are threatened in front of ATMs, and the PIN security feature is useless in these instances.

III. LITERATURE SURVEY

In 2021 Edwin Raj, Aravindh.R, Abhishek S and K,Soundari DV published a paper entitled Enhanced Security Feature of Atm's Through Facial Recognition.For the benefit of the user, this study recommends adding the face recognition features with the current existing conventional way. The Adaboost facial recognition algorithm has a 75% success rate, whereas the eigenfaces methods have an 80% success rate.. The biggest restriction of this system is that it does not overcome extra security features, and it also necessitates camera maintenance on a regular basis. In this approach, twins can be an exception. Photos can be used to get around security in some circumstances.

In 2015 Mohsin Karovaliya, Sharad Oza and Saifali Karedia published a paper entitled Enhanced security for ATM machine with OTP and Facial recognition features.This study provides a face recognition algorithm based on Eigenface. The algorithms utilised in prior systems are examined in this system. The Principal Component Aanalysis - based approach is more reliable, faster and requires less storage space. The biggest disadvantage of this system is that it can be tampered with by using user photographs. This system can be enhanced by using face masks of 3D shapes, but 3D mask production is highly expensive.

In 2015 C. Bhosale, C. Jadhav and P. Dere created a project entitled ATM security using face and fingerprint recognition.Curvelet transform is used to recognise finger prints by calculating the Euclidean distances between the 2 associated fingers code. The test of the fingers code is compared to the whole database of fingers code. If the two numbers match, an One Time Password will be delivered to the matched registered cell phone. For preprocessing, MATLAB's built-in functionality 'imread' is employed. By slightly altering the intensity distribution on a histogram, the histogram equalisation method increases the global contrast of an image. This increases the contrast in low-contrast places without impacting the overall contrast. Histogram equalisation is used to do this, it only distributes the mostly common strengthened value. The curvelet transform and Fast Fourier Transform can be used to extract functions.

In 2018 Manoj V , Sasipriya S, M. Sankar R, U. Devi E and Devika T published a paper entitled as Multi Authentication ATM Theft Prevention Using iBeacon.In this study, the ATMs security is improved by using a GSM module to generate OTP. When GSM technologies fail, this system connects to the ATM using Bluetooth, which generates an One Time Password relationship from user's mobile phones. Because no subscriptions to an SMS or email service providers is necessary, G S M modems must be a quick and simple method to get begined with SMS. With the appropriate connection and softwares, the GSM modems can also be a conventional GSM mobile. A normal GSM phone can be used as a GSM modem if it has the requisite cables and software drivers to get connected to a serial port or Universal Serial Bus port.

IV PROBLEM STATEMENT

Because the PIN is static, it is simple for thieves to obtain it from consumers by hacking or even brute force. As a result, the ATM's existing security mechanism is useless in preventing fraud. Scanning the magnetic strip on ATM cards will reveal all of the card's information. The cards become duplicated as a result of this. In some regions, people are threatened in front of ATMs, and the PIN security feature is useless in these instances. The burglar obtains

the PIN and performs the transaction, causing the security system to fail. Anybody who knows the PIN can use the card for transactions and complete them without the account owner's approval. There are no additional security measures in place to prevent the fraudulent actions.

V PROPOSED METHODOLOGY

ATMs have become an unavoidable part of our daily life. This ATM system changed the way people transacted money. For a simple cash withdrawal, there were no big lines in front of the bank. The number of ATMs a bank has can be a factor in determining a bank's strength. As the number of ATM machines grows, so does the quantity of fraudulent transactions. In our proposed system we are considering 3 cases and solution has been found. The 3 cases are:

- **The ATM machine is being used by the user as himself.**

While a single person uses an ATM, the debit card should be first inserted. The user's image is now captured via a camera. The image that was captured is now compared to the image that was saved in the data base. If the both images match (Eigenface recogniser algorithm handles the face comparison), the communication is correctly verified. The user must now input the Personal Identification Number. If the Personal Identification Number entered is right, you can proceed to the next step.

- **If the user is intimidated by someone who wants to take money from him or her without his or her consent.**

Someone is threatening the user for money. We have a solid solution for this problem. The user's face will be matched first. Now, in order to input the correct PIN, the user needs do so in reverse order. The police portal, which is on the backend, receives an
alert as a result of this. If the transactions went smoothly, the police portal would be inactive. The alert is received if the reverse order PIN is entered.

- **If a user's companion uses user card for transaction.**

When a user's companion or family member use the debit card, two image(face) ids of the user's companion are kept in the database, allowing them to complete the transaction without difficulty; however, if users companion or family members is not one of those two, there will be no match for the face. We presented a comprehensible methodology in this circumstance. In the mobile app, the user must accept their transaction. This should be done for every transaction, and the transaction can only be completed with the user's approval. The ATM software is connected to the mobile app of the user to REST API techniques. REST API are the application programming interfaces which are nothing but the bridges between the software's or applications. The debit card user must priorly inform the account holder about the transaction so that he can approve the transaction of the debit card user.

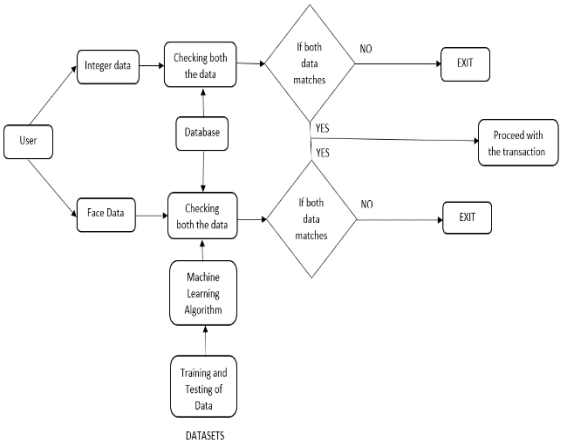


Fig.1 Architecture of ATM fraud detection and enhancing security.

System design is an application model that depicts the structure's evolution and leadership. In fig 1 it includes the framework components as well as the relationships that show how they work together to complete the overall structure. It also shows how the framework elements are connected and how they work together to complete the task. The users enters the static key id which is nothing but the PIN and his face is captured through the camera. Both the data are cross checked to each other if both data are same than the user can do the transaction or else he cannot do the transaction. The face data is checked by a machine learning model built by using eigenfaces recognizer algorithm. In this approach, a facial data point is extracted from a high dimensional imaging space, and a lower-dimensional representation is found, making classifications simple. Analyze the Principal Components (PCA), which finds the axess with the most variance, is used to find the lower-dimensional subspace. Because the axes with the greatest variances do not always include any discriminated information, classification becomes impossible.

VI ALGORITHM

In this method, A facial picture is the point in a high dimensional image space, and its representation is located in a lower dimensional space., making categorization easy. P.C.A is used to findout the lower dimensional sub space by identifying the axes with the largest variance. This transformation is good for reconstruction, but it ignores any class labels. Consider the case where the variation is due to external influences., such as light. Because the axes with the greatest variances do not always include any discriminated information, classification becomes impossible.

The algorithm works by recognizing that not all elements of a image are equally significant in recognising a faces. Instead, primary features such as the shapes of the nose, ear, and foreheads are used, and how they differ from one to another is addressed. The basic goal is to locate the area with the greatest differences. Considering that while we comparing the area of the eye and the region of the nose, there will be a significant degree of diversity. When comparing numerous faces, the comparison is made by looking for the greatest variations among the faces, which helps to differentiate the facess. This is how the Eigenface recognizer works. This algorithm's working is by looking at all of the photographs used in trainingset and extracting the main componentses that are considered significant while ignoring the rest. Principal components are the key components that serve as the primary source of information for the recognizer.

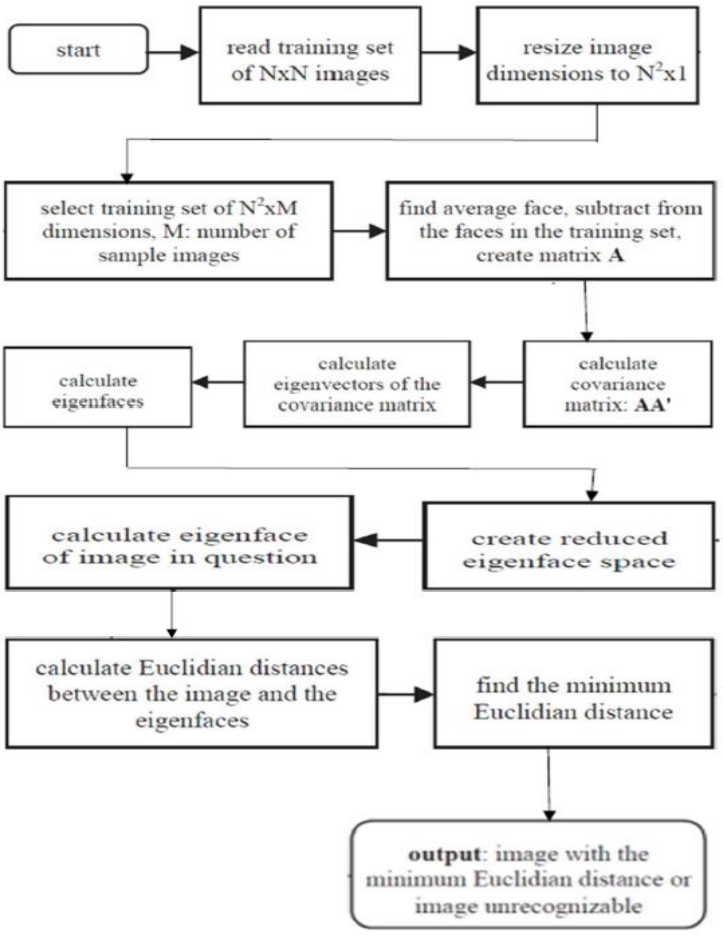


Fig.3 Working steps of the Eigenfaces method

The training images of dimensions N*N are read and translated to N2*1 dimensions as a starting point. As a result, a training set with N2*M dimensions is constructed (M denoting the number of sample images). The average of the image collection is calculated as follows:

$$\psi = {}^{1}/_{m}\, \Sigma_{i=1}^{n} \Gamma i$$

where 'ψ': average image,
'M': number of image,
'$\Gamma i'$': image vector.

The eigenface associated with greatest eigenvalue are kept. The faces space is defined by these eigenfaces. The picture is projected into the face space formed by the eigenface to create the eigenspace. As a result, the weight vectors are computed. In the pre-processing step of recognition, the image's dimensions are changed to suit the standards, and the image is enhanced. The image's weight vector is compared to the weighted vectors of the face in the data base.

Each faces in the training set is deducted from the average face. The results of the subtraction operation are used to

create a matrix (A). Each image's deviation from the average image is computed as follows:

$$\phi_i = \Gamma_i - \psi \quad i = 1,2, \dots M$$

where ϕ_i: The differences between the face data and the average picture is what it is. The covariance matrix C is generated by multiplying the transpose of the matrix generated by the subtraction operation (A):

$$C = A^T A$$

where A is generated by the differences of the vector,

i.e., $A = [\phi_1, \phi_2 \dots \phi_m]$

The matrix C has dimensions of N*N. C is made up of M pictures. C has the dimensions N*M in practice. However, because A has a rank of M, only 'M' out of 'N' eigenvector are non-zero. The covariance matrix's eigenvalue are determined.

Method	Number of images in the training set	Success rate
Principal Component Analysis	400	79.65%
Principal Component Analysis + Relevant Component Analysis	400	92.34%
Independent Component Analysis	170	tanh function 69.40%
	40	Gauss function 81.35%
Hidden Markov Model	200	84%
Active Shape Model	100	78.12-92.05%
Wavelet Transform	100	80-91%
Support Vector Machines	-	85-92.1%
Neural Networks	-	93.7%
Eigenfaces Method	70	92-100%

Table: Comparison of some work related to face recognition

VII RESULTS

After training the machine learning model a test image has been sent to test the efficiency of the build model. We have trained the machine learning model with the 440 images of face as face datasets from Kaggle website (AT&T Face Datasets). Test data is used to do a last, real-world check on an unknown dataset to ensure that the ML Algorithm was properly trained.

The processing takes to predict the image is recognized from the database. Here the model matches the testing image to the image that of is in the database.

```
n [19]: alpha_1 = 3000 #chosen threshold for face detection

projected_new_img_vector = eigenfaces[:q].T @ omega #n^2 vector o
diff = mean_subracted_testimg - projected_new_img_vector
beta = math.sqrt(diff.dot(diff)) #distance between the original f

if beta < alpha_1:
    print("Face recognized in the image! ", beta)
else:
    print("No face recognized in the image! ", beta)
```

```
Face recognized in the image!  2011.0301308707733
```

So, the eigenface recognizer is built to recognize image present in the database with the image provided by the user interface. The user interface is built using the Python's Tkinter library which contains the Graphical Library in it.

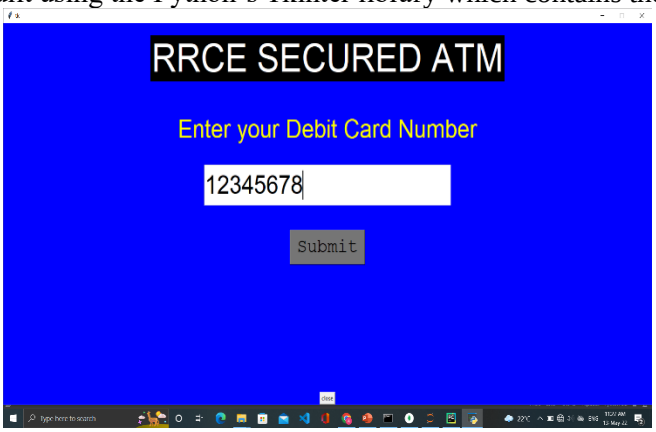


Fig 4:The above image shows the user interfacce where user will enter the debit card number.

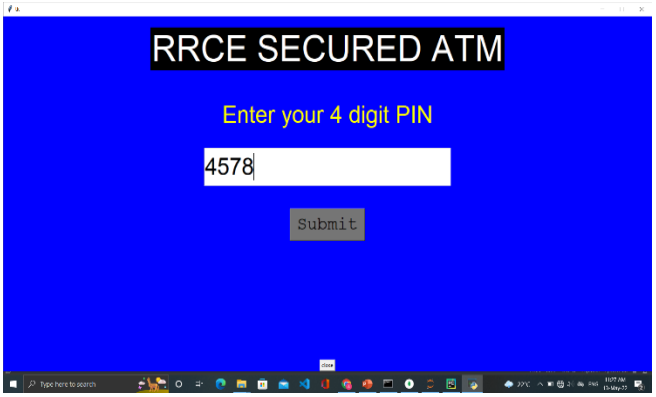
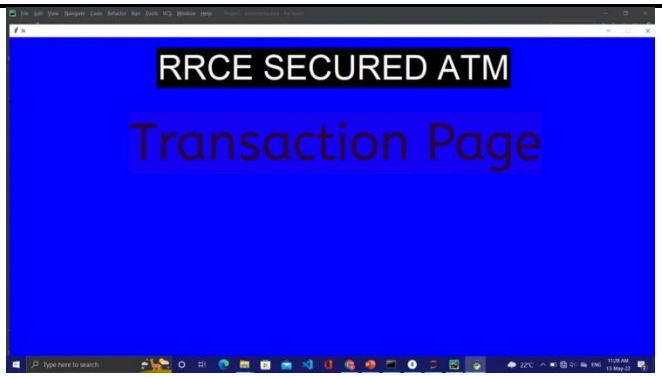


Fig 5:The above image shows the user interfacce where user will enter the PIN. When the user enters the PIN the software checks from database.

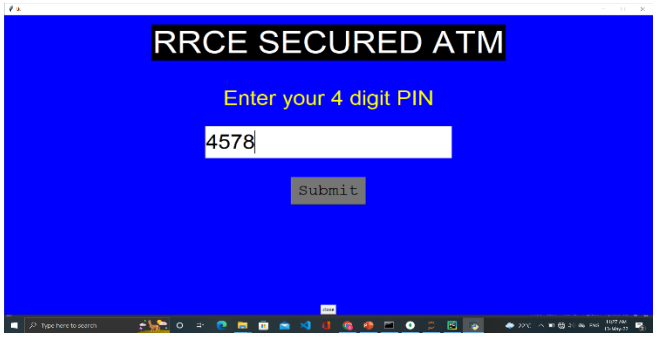
After user's PIN is verified, the user will get the two options One is to proceed to the transaction page where this option can be used only by the account holders. Second option is Not the Account Holder, if the debit card user is not the account holder than the he need to click this option where a message will be sent to the account holder to approve or disapprove the transaction of the user.

If both the options get verified than the user will be sent to the Transaction page where he can do the transaction of his choice.



If the user enters the reverse PIN in entering in the Entering the PIN page and if his Face is recognized or he recieves the permisssion from thhe user through mobile than a trigger is sebt to the poloce portal where data is stored. This happens when the debit card user is threatened by some burglar ot theif.

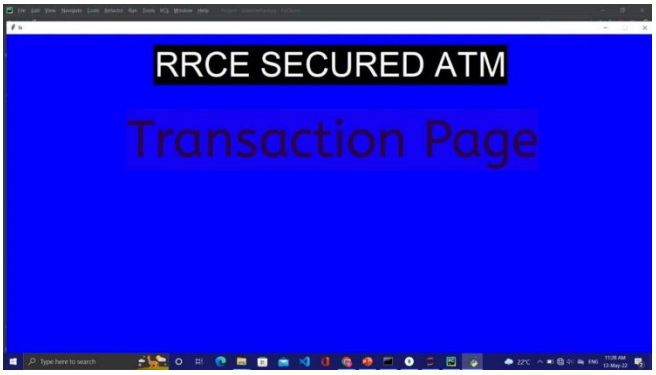
The above image shows the user interfacce where user will enter the debit card number.



The above image shows the user interfacce where user will enter the PIN. When the user enters the PIN the software checks from database.

After user's PIN is verified, the user will get the two options One is to proceed to the transaction page where this option can be used only by the account holders. Second option is Not the Account Holder, if the debit card user is not the account holder than the he need to click this option where a message will be sent to the account holder to approve or disapprove the transaction of the user.

If both the options get verified than the user will be sent to the Transaction page where he can do the transaction of his choice.



If the user enters the reverse PIN in entering in the Entering the PIN page and if his Face is recognized or he recieves the permission from the user through mobile than a trigger is sent to the police portal where data is stored. This happens when the debit card user is threatened by some burglar or thief.

VIII CONCLUSION

Finally, we can conclude that the method which we have built can increases the security features of the Automated Teller Machines and along with finding some of the Fraud and theft activities done in the ATM's. The method proposed by us is very efficient because of the usage of eigenface recognizer algorithm which has accuracy percentage of 85% when compared to the adaboost algorithm which has the accuracy percentage of 75%. The accuracy percentage is obtained by training and testing the models through a python library known as OpenCV.

This project can be improved by the installation of highly qualified camera. 3-dimentional camera should be used for the condition of twins(identical) and photo bypassing purposes. Along with regular maintenance of the cameras present in the ATM system. Providing the high security feature to the API's for communication between the account holder and the ATM when the account holder doesn't do the transaction.

IX REFERENCES

1) J.J.Patoliya, M.M. Desai, "Face Detection based ATM Security System using Embedded Linux Platform ", 2nd International Conference for Convergence in Technology (I2CT), 2017.
2) M.Karovaliyaa, S.Karediab, S.Ozac, Dr.D.R.Kalbande, "Enhanced security for ATM machine with OTP and Facial recognition features", International Conference on Advanced Computing Technologies and Applications (ICACTA), 2015.
3) Sivakumar T. 1 , G. Askov 2 , k. S. Venuprathap, "Design and Implementation of Security Based ATM theft Monitoring system", International Journal of Engineering Inventions, Volume 3, Issue 1, 2013.
4) C. Bhosale, P. Dere, C. Jadhav, "ATM security using face and fingerprint recognition", Interna-tional Journal of Research in Engineering, Technology and Science, Volume VII, Special Issue, Feb 2017.
5) Manoj V, M. Sankar R , Sasipriya S , U. Devi E, Devika T , "Multi Authentication ATM Theft Prevention Using iBeacon", International Research Journal of Engineering and Technology *(IRJET)*.
6) Wang,H. Ji, Y. Shi, " Face recognition using maximum local fisher discriminant analysis",18th IEEE International Conference on Image Processing, 2011.
7) K.Shailaja and Dr.B.Anuradha, "Effective Face Recognition using Deep Learning based Linear Discriminant Classification ", IEEE International conference on Computational Interlligence and Computing Research,2016.
8) H. R. Babaei, O. Molalapata and A.H.Y Akbar Pandor, "Face Recognition Application for Au- tomatic Teller Machines (ATM)", International Conference on Information and Knowledge Management (ICIKM),2012.
9) Chen, Joy Iong Zong. "Smart Security System for Suspicious Activity Detection in VolatileAreas." Journal of Information Technology 2, no. 01 (2020): 64-72.