An Integrated Reinforcement DQNN Algorithm to Detect Crime Anomaly Objects in Smart Cities

Dr. Jyothi Mandala[1]
Assistant Professor
Department of CSE, School of Engineering & Technology, CHRIST (Deemed to be University), Bengaluru, India

Pragada Akhila[2]
Assistant Professor
Department of CSE, Gayatri Vidya Parishad College of Engineering (A) Visakhapatnam, Andhra Pradesh, India

Vulapula Sridhar Reddy[3]
Assistant Professor
Department of IT, VBIT
Telangana, India

***Abstract*—In olden days it is difficult to identify the unsusceptible forces happening in the society but with the advancement of smart devices, government has started constructing smart cities with the help of IoT devices, to capture the susceptible events happening in and around the surroundings to reduce the crime rate. But, unfortunately hackers or criminals are accessing these devices to protect themselves by remotely stopping these devices. So, the society need strong security environment, this can be achieved with the usage of reinforcement algorithms, which can detect the anomaly activities. The main reason for choosing the reinforcement algorithms is it efficiently handles a sequence of decisions based on the input captured from the videos. In the proposed system, the major objective is defined as minimum identification time from each frame by defining if then decision rules. It is a sort of autonomous system, where the system tries to learn from the penalties posed on it during the training phase. The proposed system has obtained an accuracy of 98.34% and the time to encrypt the attributes is also less.**

***Keywords*—HybridFly; Advanced Encryption Standard (AES); reinforcement; anomaly detection; crime rate prediction; security attacks; RCNN**

I. Introduction

Anomalies always refer to the abnormalities or deviations that occur in regular flow. Since, all the devices in the IoT are arranged in the distributed network manner, the implementation of anomaly has its impact on the designed system in terms of root cause analysis detection, cost and threat reduction. The various kinds of mechanisms that can identify anomaly are discussed in Fig. 1.

The Visual Discovery is the trending approach for anomaly detection process, where IoT connected video surveillances is connected in network. During this process, huge amount of data are captured and it is difficult to work on those data streams with high and multi-dimensions. So, an anomaly marker system is developed, in which threshold is marked with the help of neighborhood estimation. So, an anomaly marker system is developed, in which threshold is marked with the help of neighborhood estimation.

In this existing system, the visualization process helps to form the segments which are occasional and peculiar and it also finds the correlation between different entities that are captured in the data streaming process with in the marked area of regions. The threshold values in this mechanism are dynamic in nature, which are automatically adjustable based on the application data in the marked region. But, the system suffers with unbalanced noisy data.

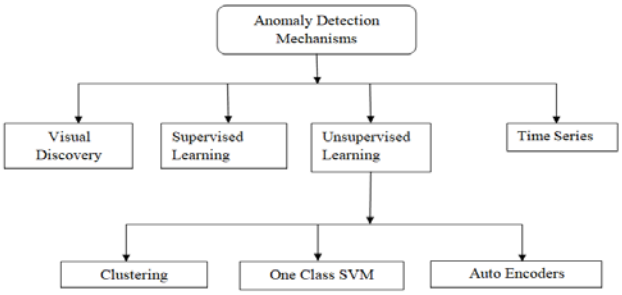

Fig. 1. AD Mechanisms for Crime Predictions.

II. Literature Survey

In [1] the primary goal of an abnormality vulnerable model is to classify the system's characteristics into usual and untruthful behaviors. To assess the tendency of occurrences, smart city managers must use anomaly observation engines to safeguard information from being compromised by flaws or breaches. This paper focused on conducting an analogy of various ML methodologies over DNN by performing a research study to identify the best method that can work with abnormalities in data. This study has chosen the issue of attack type by the rarity in IoT. This study was carried out on various attacks that may occur by the abnormalities and an entire study was made out. The researchers have also developed a grid structure that can determine the various types of interventions and foresee the possibility of happening an intrusion. This research helps in choosing the best methodology for others to perform with their own study from the proposed method depending on their issue as this study explains each method that was used layer by layer.

In [2] an innovative and expert motive that was developed to help in the growth of the resources or for the people using the advanced technologies that connects various electronic gadgets like sensors and work on together by generating a cumulative output is the development of smart cities. This amazing development was deployed in most of the places round the globe, but to make the devices derive better precise

values that helps in yielding best accurate outcomes and to make the developed machine more reliable, DL concepts were opted. This paper relies on various DL techniques and derives a cumulative study depending on the structural enhancement on the smart city information. Along with the usage of these preferred technologies, their usage, utilizations, and post enhancements were also explained.

The standard methodologies used to deploy the values that usually deviate out from the actual information, but it will be useful in some conditions, with mathematical strategies [3]. Such type of data also satisfies a few constraints so that ignoring this information paves data loss. This data can also be included to make the machine perfect. So, these papers focused on deploying a method that trains itself given a condition with all the possibilities available and learn from its experience. This method has shown better results in gaming, as stated and to promote it to next level, this model was applied in real time. This model was deployed and compared with those outcomes of ML techniques with various performance calculations and stated that their neural grid has derived more precise results with less issue and keep tracking of all the abnormalities.

With the increasing growth of intellectual areas and connecting the electronic devices the information is gathered and is shared among the united devices which lead in misleading of the information and exposure of risks is high [4]. So, rather than focusing on the raising technologies, advancing the growth of security devices or systems, analyzing them continuously and to eradicate the unnecessary conditions are also critical. For this issue, ML methods were opted to identify the rate of efficiency of the services provided within the intelligent city with security problems. The researchers have developed a self-learning system that learns from the given constraints or the past experiences from the information that supervises the overall activities that were organized. A neural grid examines the incoming activities and identifies the suspicious activities by breaking down them into chunks of parts since it reduces the difficulties and enhances the performance of the grid.

The problems that may rise due to the connectivity of electronic devices within an intellectual city are as similar as those that arise in an intelligent home rather on a smaller scale, but the risks that may occur to the associated accessories with security and for handling of the information [5]. The consequences of a security flaw are not restricted to online; it could also influence or be assisted in spatial context, for as by speech. Vulnerability assessment in this ecosystem should not rely only on estimation methods that retain the same throughout times and for all participants. The researchers have presented a system that automatically adjusts to is ecosystem whenever a new commodity is introduced that also distinguishes the necessary abnormalities. This method was induced in a reward technique to its attributes under its related ecosystem of untagged data and finds the anomalies.

With the rise in advanced technologies and their applications in real life have changed into a smarter life like form urban areas to intellectual cities [6]. This also helped in usage of various sources and services in hand to very common people as well. But even these advancements have challenges, one of which is power issue. These electronic devices needed to be associated with the commodities and should always be in a communication in share but have limited power storage devices along with the issues in networks and information protection. This paper deployed a statistical self - learning model that focuses on avoiding the DDos aggression on IoT accessories and their networks. These models were deployed based on the correlations of the various models within the layers of the network grids that also focuses on the security uncertainties.

Recently, advancements in connecting the intellectual accessories have improved with various type of grids and development [7]. One of such enhanced topologies with a harmonized structure was implemented in WMN which had derived several powerful attributes for development of the intelligent smart grids NAN with the advancing research on the devices that record the capabilities, working and usage of a smart system. With the raise of such systems, the uncertainties that may happen have dragged the scientist's attention with are related to ignorance of uncertainties. To find those abnormalities patterns, a model that finds out them locally on each site was established throughout the power distinguished model. A self-learning technology with block chain was developed to associate the local patterns of the outliers on a larger image.

The advancements in the connected system under a single ecosystem model were increased regularly and are in a great demand in multiple fields to its varied applications [8]. But increasing technologies also increases that risks with those related to various modules in between. The recent advancements in ML with named or tagged data for distinguishing the objects have helped in reaching out the problems. Detecting the attacker is one of the major problems when dealing with protection of devices in association. This paper has established a methodology focusing on this issue with a model that learns by itself based on the given attributes, constraints set and information of past. This method on working on the same data iteratively develops itself and can distinguish a risk or suspicious action when it is introduced. This research was applied to a live data with tagged names and stated that it has shown a better performance in contrasting with ML models.

The study of 19 unsupervised anomaly detection algorithms is with evaluation for multiple domains [9]. These evaluations focused on strengths and weakness of different approaches. This research is applied on 10 different datasets which is focused on global/local anomaly behaviour on real-world applications.

Prevention from cyber-attacks is very much needed for secure operation [10]. This research paper is about online anomaly detection problem which mentioned a solution for this using model free reinforcement learning. The results generated by this approach show the timely and accurate prevention by detecting the cyber-attacks which are targetting on smart grid.

III. Proposed Methodology

To reduce the crime rate in the smart cities, the proposed system has developed an anomaly detector integrated with reinforcement techniques especially in the remote places during the mid-night hours. The Fig. 2 represents different data frames associated with fire crime accident happened at a business location.

Fig. 2. Fire Accident Captured in Video Surveillance.

Proposed system works on the dataset known as "UCF-Crime Anomaly", which has multi cases video captured records of different crime incidents occurred in various locations in India. The major goal of this system is to identify the criminals and also sends notification to the nearest police station about the incident. The reinforcement technique helps the model in identifying the multiple objects simultaneously and generates a sequence of actions by generating the dynamic rules based on the captured entities. The overall experimental setup is illustrated in Fig. 3.

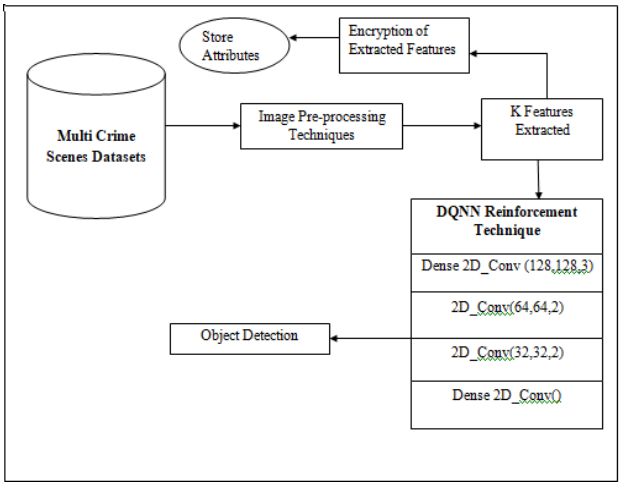

Fig. 3. Object Detection Process in Crime Anomaly Detection.

The proposed model, starts processing the objects and persons captured by the video by finding the facial land marks for the persons and RCNN for the objects. The proposed model uses traditional processing techniques like brightness and geometric transformation.

In brightness transformation, it implements histogram equalization to enhance the quality of the pixels it uses cumulative distributive frequency and produces normalized histogram. The reason for selecting histogram equalizer is it is efficient in dealing non-monotonic and non-linear structures. The crime scene contains more number of dissimilar and complex structured figures. So histogram equalizer is the apt brightness technique. In geometric transformations, the proposed algorithm majorly focuses on interpolation based on Grey scale factors. The change of direction or enhancements to the images produce new co-ordinates, these values may not be accommodated. The system needs interpolation mechanism to fit these new co-ordinates system. The proposed system implements linear interpolation technique, in which the neighboring pixel values are examined and considers the value with maximum brightness function as output.

Then for the person identified images are fine tuned to remove the noisy data during the capturing process and extract the important features. The proposed system uses the concept of dynamic fly to select the adaptive features and extract the needed features. The concept of genetic algorithm is opposite to the correlation because the attractiveness property states that distance have inverse impact on the attraction. The extracted features are encoded using Hybrid Fly algorithm to protect the information for further mishandling by the attackers or hackers.

Algorithm: Pseudocode for Attribute Encryption using Hybrid Fly Algorithm:

Begin

1. Define an objective function of K-extracted dimensions
2. Set up initial dimensions as firefly population, k
3. Determine the intensity for each firefly group based on the threshold
4. for each i 0 to k
5. for each j 0 to i

i. if (F[i]>F[j])

Then update the firefly to next fold

ii. Else

Calculate attractiveness distance based on the threshold

iii. best_feature[i] Update rank value for each feature by finding the best score

6. new_feature AES(best_feature[i],key=256)

End

In the proposed system, model free Deep Q-Learning Neural Network(DQNN) technique is implemented by defining an action value function in terms of current state and action to be performed on the current state by the agent based on the rules generated by the AO* algorithm. The major goal of this NN model is to maximize the rewards in every iteration

so that the time to detect the object decreases. The reward function is defined as shown in (1).

DQNN(S_New, A_New)←R(S_New,A_New)+α* max(S_old,A_New) (1)

In every iteration DQNN, updates the table associated with state and action. The states are passed as input to the neural network, which is designed as the auto encoder. All the Q-values are obtained as continuous output. The "tanh" activation helps the regressor in predicting the output variable. The output of the objection is represented in Fig. 4.

Fig. 4. Person Identification in Crime Scene.

For object detection, the CNN creates the feature map based on the selective search to create new regions of interests in the network. The visual attention mechanism helps the system to consider the weighted average mechanism, to obtain the new vectors.

IV. Result and Discussion

The proposed system to prove its efficiency, it has performed a comparative study on the different existing mechanisms and is illustrated in Fig. 5.

Fig. 5 represents different algorithms compared on the x-axis and accuracy percentages on the y-axis. There is a clear evidence that proposed model has exhibited best accuracy among all the others. The model has also obtained recall and precision values in terms of identifying the true positive and false negative labels. The model also discusses the comparison based on the encryption time of different security algorithms and the proposed algorithm and is illustrated in Table I.

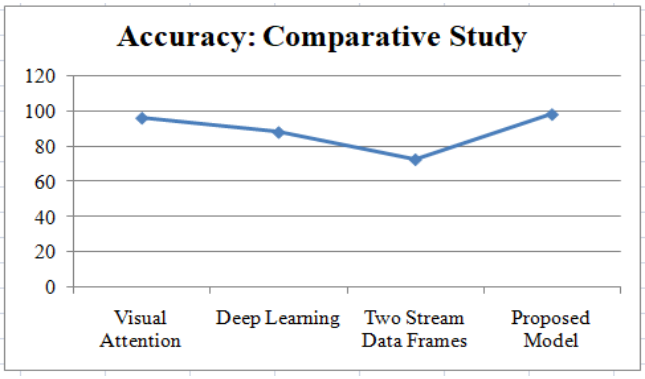

Fig. 5. Fire Comparative Study on Accuracy in Predicting the Object Detection.

TABLE I. File Encryption Time

S.No	Input Size in MB	RSA	DES	Proposed
1	25	0.485	0.41	0.334
2	50	0.535	0.443	0.352
3	75	0.563	0.499	0.431
4	100	0.625	0.542	0.46

In Fig. 6, X-axis represents size of the file in MB as mentioned in Table I and Y-axis represents time in nano seconds.

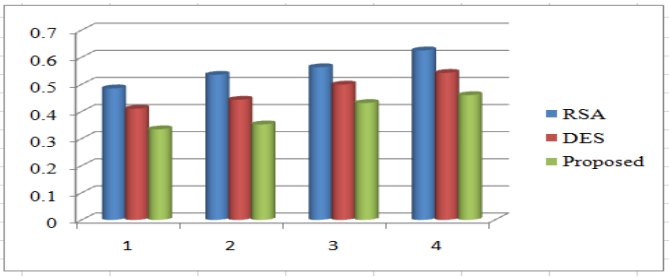

Fig. 6. Encryption Time- Comparative Study.

When compared to RSA and DES algorithms, proposed algorithm has got less time to encrypt the file and the encryption time increases when the file size increases. This description is illustrated in Fig. 6.

V. Conclusion

With the reinforcement technique it is observe that high precision and accuracy values are obtained with very short training of the system. One of the advantages of the proposed system is assigning ranks to the peculiar objects that has been captured and also reduces the ranking losses that incur due to the miss-classification of the objects. The background subtraction process helps the system to improve the quality of the software and integrated visual attention mechanism can also works fine in identification of moving objects. The involvement of the computer vision has enhanced the quality and training phase automatically without any human intervention. The proposed system has implemented model free technique because it consumes less space, since it does not involve any storage of states and actions but it applies brute forces techniques. So, the knowledge updation is time consuming task. In the future work, research can be extended based on the time lines and historical data that happened frequently in the span of time which involves model based techniques.

References

[1] Reddy, D. K., Behera, H. S., Nayak, J., Vijayakumar, P., Naik, B., & Singh, P. K. (2020). Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities. Transactions on Emerging Telecommunications Technologies, 32(7). https://doi.org/10.1002/ett.4121.

[2] Bhattacharya, S., Somayaji, S. R. K., Gadekallu, T. R., Alazab, M., &Maddikunta, P. K. R. (2020). A review on deep learning for future smart cities. Internet Technology Letters. https://doi.org/10.1002/itl2.187.

[3] Zhou, K., Wang, W., Hu, T., & Deng, K. (2021). Application of Improved Asynchronous Advantage Actor Critic Reinforcement

Learning Model on Anomaly Detection. Entropy, 23(3), 274. https://doi.org/10.3390/e23030274.

[4] Zhang, Mengqi et al. 'Machine Learning Techniques Based on Security Management in Smart Cities Using Robots'. 1 Jan. 2021 : 891 – 902.

[5] R. Heartfield, G. Loukas, A. Bezemskij and E. Panaousis, "Self-Configurable Cyber-Physical Intrusion Detection for Smart Homes Using Reinforcement Learning," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1720-1735, 2021, doi: 10.1109/TIFS.2020.3042049.

[6] Ashraf, J., Keshk, M., Moustafa, N., Abdel-Basset, M., Khurshid, H., Bakhshi, A. D., & Mostafa, R. R. (2021). IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities. Sustainable Cities and Society, 72, 103041. https://doi.org/10.1016/j.scs.2021.103041.

[7] Belhadi, A., Djenouri, Y., Srivastava, G., Jolfaei, A., & Lin, J. C.-W. (2021). Privacy reinforcement learning for faults detection in the smart grid. Ad Hoc Networks, 119, 102541. https://doi.org/10.1016/j.adhoc.2021.102541.

[8] Q. -V. Dang and T. -H. Vo, "Studying the Reinforcement Learning techniques for the problem of intrusion detection," 2021 4th International Conference on Artificial Intelligence and Big Data (ICAIBD), 2021, pp. 87-91, doi: 10.1109/ICAIBD51990.2021.9459006.

[9] Goldstein, M. Uchida, S. "A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data." PLoS ONE 2016, 11, e0152173, doi: https://doi.org/10.1371/journal.pone.0152173.

[10] Kurt, M.N., Ogundijo, O.; Li, C., Wang, X. "Online Cyber-Attack Detection in Smart Grid: A Reinforcement Learning Approach." IEEE Trans. Smart Grid 2018, 10, 5174–5185. doi: https://arxiv.org/ct?url=https%3A%2F%2Fdx.doi.org%2F10.1109%2FTSG.2018.2878570&v=17393103.