**Title:** Detecting cyber attacks in smart cities by a deep learning model

**Aim:** This paper discusses the application of deep learning model to detect and mitigate common cyberattacks in smart cities. Through various networks of the deep learning model, cyberattacks like fraud, malware, phishing, etc are detected based on the input given to the networks and the characteristics patterns predict the next likely scenario. This would make it easier to detect and mitigate such attacks.

**Keywords**: Smart city, Deep learning model, Cyber attacks, Neural networks.

**Introduction:**

"Smart city" is a place where social facilities, commercial infrastructure, information technology infrastructure, and also physical framework are all interconnected to increase the combined intelligence of the area (V et al., 2018). Primarily, the goal of smart cities has been to transform people's lives through a variety of improvements. Secondarily, though smart cities improve quality of life and provide many benefits, there are also additional undetected risks to cyber safety, such as data leaks and malicious intrusions. The rapid adoption of global smart city technologies is outpacing the present technological growth, thus an appropriate architecture founded on deep learning methods is crucial to defend smart cities. In addition to covering current relevant work on IoT safety in smart cities, this paper highlights the comprehension and application of the concepts of Smart Cities (SC), Cyber Security (CS), and Deep Learning (DL). In particular, we studied a number of deep learning models, including generative adversarial networks, restricted Boltzmann machines, deep belief networks, recurrent neural networks, and convolutional neural networks, among others.

**Literature review:**

According to Al-Saidi and Zaidan (2020), smart cities are vast, complicated, and reliant on a variety of technologies that present a number of technical, economic, political, and social problems. Although creating smart cities has advantages to support residents, businesses, the environment, etc., these cities are vulnerable to multiple privacy and security threats, which makes it challenging to establish an administrative maturity in them (Baig et al., 2017). In a smart city, a single negligent move by a person or institution might endanger the entire community (Zhou et al., 2021). A significant difficulty for digital court investigations is this complicated city. Information and the framework must be protected from cyber-crimes and illegal activity in order to ensure security in a smart city (Sengan et al., 2020). Deep learning, a sort of machine learning and artificial intelligence (AI), has various benefits in the smart city and really resembles how an individual learns specific topics (Atitallah et al., 2020). Deep learning can assist the system adapt to new environments by continually gathering and monitoring data (Singh et al., 2020). Machine learning and neural networks both gain from the use of deep learning, a subfield of artificial intelligence (AI). Artificial intelligence programmes have recently significantly improved in various fields, such as robotics, artificial language processing, and many others, as compared to traditional machine learning approaches (Belhadi et al., 2021). To attempt to mitigate or restrict the impact of these obstacles, this study will identify and examine the cyber security issues that smart cities are facing (as per deep learning). Modern systems have numerous advantages, but it also has significant hazards and flaws in the personal-cyber infrastructure. Several risk factors exist in the primary personal-cyber infrastructures that affect urban infrastructure, such as the supply of electricity and water, as well as streets, buildings, etc. Cameras, communication networks, building management systems, and transportation management systems are just a few of these parts and systems. Ijaz et al. (2016) separated communication privacy difficulties from corporate privacy issues. Eavesdropping, denial of service, malicious manipulation and assaults, route attacks, detection, and secondary usage were among the difficulties to communication privacy. In addition, frauds and attacks on data integrity were presenting company privacy issues. In-depth insights on digital smart city surveys and a complete picture of the security situation in smart cities were presented by Baig (2017). Researchers discovered security issues with city infrastructure such as smart grids, automated building system security, drone protection, smart cars, IoT sensors, and cloud storage.

**Methodology:**

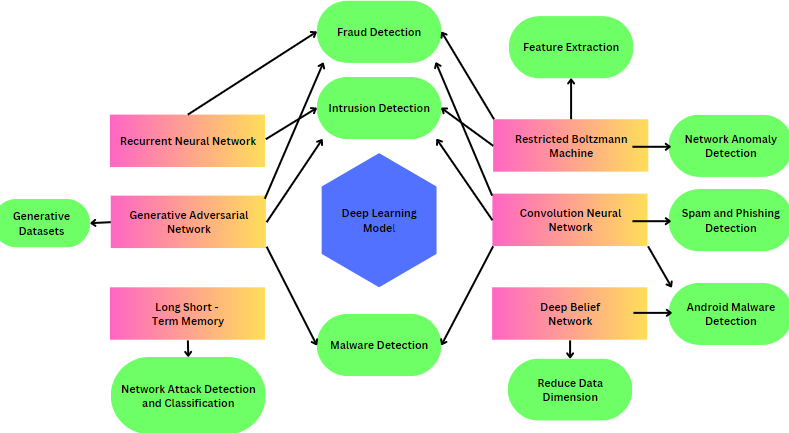


Figure 1: Deep Learning Model Application in Smart City

The infrastructure is equipped with recurrent neural networks for fraud and intrusion detection. By identifying recurring patterns of transactional activity in the data set, recurrent neural networks can identify fraud. Recurrent neural networks are renowned for their quick processing and responsiveness. Recurrent neural networks for intrusion detection are able to stop incidents from happening in the first place by identifying certain trends that hackers choose. Recurrent neural networks are used in intrusion detection systems to forecast upcoming assaults, such as zero-day attacks, and to get ready for mutant attacks by their artificial signatures. Recurrent neural networks must be used to create dangerous datasets comprising historical malicious software signatures and currently common malware variants in order to do this. Recurrent Neural Networks (Recurrent neural networks), which are memories-based, faster computational neural networks, are enhanced by the Long Short-Term Memory (Long Short-Term Memory) approach, which is employed in this study to create a deep learning intrusion detection model. In smart cities, long-short-term memory is used for network attack detection and categorization. The network can function as a sensor by using OPenflow in Long Short-Term Memory to examine the characteristics of the traffic moving across the network and spot hose assaults.

In this case, generated data sets, intrusion detection, and fraud detection are all handled by generative adversarial networks. Generative Adversarial Networks are all-purpose, adaptable, and potent generative deep learning models that have succeeded in creating compelling, realistic-looking pictures.

Existing fraudulent activity is input into the Generative Adversarial Network, and the result is an elevated set of training information that produces the original data, which includes the classifier's sensitivities. Because of its tremendous potential for learning complicated, high-dimensional actual data distribution, generative adversarial networks are employed in intrusion detection. Generative Adversarial Networks perform better for IDS in attack detection and model stability when compared to conventional deep learning approaches. Malware threat levels, damage estimates, and malware family categorization are used to efficiently identify and remove malware using a generative adversarial network. In order to create artificial data that may be utilised to provide datasets for the network in smart cities, generative adversarial networks are employed. These datasets can be utilised to provide artificial signatures of malicious attacks or user information.Deep Belief Networks are probabilistic generative models made up of several layers of latent stochastic parameters. To identify malware in androids, a Deep Belief Network and a back propagation neural network classifier are built. To identify fraudulent mobile applications, the Deep Belief Network-BP model is trained on several API properties. The contrastive divergence strategy, which floors the data likelihood with regard to the model parameters to quality of the non-linear dimensionality reduction, is the current method for Deep Belief Networks. A Deep Belief Network with two layers may be used to visualise data dimensions. The first one corresponds to the reduced dimensionality space while the other layer is made up of concealed variables.

Convolutional Neural Networks has the ability to extract features in the computer's vision to adapt constantly in any changing environment. Hence they are highly used in remediating cyber crimes in any environment. But in this smart city it is used for fraud, malware, intrusion, android malware, spam and phishing detection. S.Ghosh() used neural network algorithms to construct a transaction fraud detection. A.I.Kokkinaki() used clustering methods to analyse the distinction between normal or abnormal transactions. Malware detection in cyber cities are detected by Convolutional Neural Network with detecting malware in source code and binary code. Network administrators have found it 90% accurate in identifying malware so that they are mitigation techniques and tools in place for a potential malware attack. Convolutional Neural Network can automatically extract effective complex features making it easy to create an intrusion detection system. Within a network cyber criminal signatures are analysed by Convolutional Neural Network. Malicious applications in mobile devices can gain access to sensitive and crucial personal or professional information by exploiting unsolicited permission controls. The method investigated permission patterns based on Convolutional Neural Network with a data set of android applications which might have malware code in their source code or through ads in the application.Email classification techniques are embedded to Convolutional Neural Network using well-describing features extracted from benchmark datasets. The training of the accuracy and validation features is employed in Convolutional Neural Network architecture to detect spam and phishing emails.

Restricted Boltzmann Machine, a network of stochastic neurons behaving according to an energy-based model. These networks couple the ability to express much of the variability of data, given by generative models, with the good classification accuracy derived from discriminative classifiers.

It is used for fraud, feature, intrusion, and network anomaly detection. Intrusion detection is done by Restricted Boltzmann Machine which takes byte level raw data as input without feature engineering. Distributed embedding is utilised to preprocess network data to make it more suitable for deep neural networks. Fraud detection is done by the Discriminative Restricted Boltzmann Machine by combining the expressive power of generative models with good classification accuracy capabilities,which derived part of its knowledge from incomplete training data. The ability of Restricted Boltzmann Machine to adapt to change and generalise its behaviour to multiple different network environments and train with general traffic inorder to detect an intruding hacker with suspicious traffic. Feature extraction is done by combining the existing features in the data set and transforming them into a concise set of features that can be used for clustering, classification, and other tasks. Desirable characteristics of an effective model for network anomaly detection systems are adopted to implement semi- supervised anomaly detection system. As attack techniques and patterns change, previously gained information of the traffic flow must be constantly changed.

**Evaluation:**

**Conclusion:**

In this report, two important and complex issues, including privacy and cyber-security in the smart city were examined. A review of the research literature in the field of smart cities found that some studies have provided useful guidance for policymakers and city managers who sought to better define and implement smart city strategies and operational plans. Other studies have described the architecture of deploying and testing the deep learning model in the smart city to provide a platform for testing and evaluating concepts on a large scale under real-world conditions. Smart cities are a new kind of integration of information and communication technologies. By connecting and integrating systems, the rate of attacks and vulnerabilities will increase. Therefore, it is important to provide solutions with a focus on sustainable cyber security and risk reduction strategies. The research in this study showed that … **References:**

Ma, C. (2021). Smart city and cyber-security; technologies used, leading challenges and future recommendations. Energy Reports, 7. doi:<https://doi.org/10.1016/j.egyr.2021.08.124>.

Chen, D., Wawrzynski, P. and Lv, Z. (2020). Cyber Security in Smart Cities: A Review of Deep Learning-based Applications and Case Studies. Sustainable Cities and Society, 66, p.102655. doi:<https://doi.org/10.1016/j.scs.2020.102655>.

Ullah, Z., Al-Turjman, F., Mostarda, L. and Gagliardi, R. (2020). Applications of Artificial Intelligence and Machine learning in smart cities. Computer Communications. doi:<https://doi.org/10.1016/j.comcom.2020.02.069>.

Rashid, Md.M., Kamruzzaman, J., Imam, T., Kaisar, S. and Alam, M.J. (2020). Cyber Attacks Detection from Smart City Applications Using Artificial Neural Network. [online] IEEE Xplore.

‌Bhardwaj, T., Upadhyay, H. and Lagos, L. (2021). Deep Learning-based Cyber Security Solutions for Smart-City: Application and Review. Learning and analytics in intelligent systems, pp.175–192. doi:<https://doi.org/10.1007/978-3-030-85383-9_12>. ‌

Rashid, M.M., Kamruzzaman, J., Hassan, M.M., Imam, T. and Gordon, S. (2020). Cyberattacks Detection in IoT-Based Smart City Applications Using Machine Learning Techniques. International Journal of Environmental Research and Public Health, [online] 17(24), p.9347.

Dodge, M. and Kitchin, R. (n.d.). THE CHALLENGES OF CYBERSECURITY FOR SMART CITIES. [online] Available at: <https://personalpages.manchester.ac.uk/staff/m.dodge/Dodge_Kitchin_Challenges_of_Cybersecurity_for_Smart_Cities.pdf>.