The International Journal of Research, Education, and Innovation (IJREI)
Volume 1, Issue 3, May 2024, pp.7-11

Review of Theft Detection Algorithms for Smart Security Systems

[1] Sonawane Rahul Shivaji, [2] Jeetendra Singh Yadav

[1]M. Tech., Scholar, CSE Bhabha University Bhopal, India

[2]Assis. Prof., CSE Bhabha University Bhopal , India

Abstract- *This review paper provides a comprehensive analysis of various theft detection algorithms implemented in smart security systems. With the increasing integration of artificial intelligence and machine learning into security technologies, the ability to accurately detect and prevent theft has become a critical focus. This paper examines a range of algorithms, including traditional methods and advanced machine learning approaches like neural networks, decision trees, and ensemble models such as XGBoost.*

The review highlights the strengths and limitations of each algorithm in terms of accuracy, precision, recall, and overall effectiveness in real-time theft detection. It also discusses the challenges faced in implementing these algorithms, including data quality, computational complexity, and the adaptability of models to different environments and scenarios. Through this analysis, the paper aims to identify the most promising theft detection algorithms and propose directions for future research to enhance the capabilities of smart security systems.

Keyword: Theft Detection, Smart Security Systems, Machine Learning, Neural Networks, XGBoost, Algorithm Performance, Artificial Intelligence, Real-time Detection, Security Technology

1. INTRODUCTION

In an era where technology permeates every aspect of daily life, the need for robust security systems has become increasingly critical. Smart security systems, powered by advanced algorithms and artificial intelligence, are at the forefront of this technological evolution, offering enhanced protection against theft and other security breaches. These systems utilize various sensors, cameras, and interconnected devices to monitor environments in real-time, providing instant alerts and responses to potential threats.

The effectiveness of a smart security system is largely determined by the algorithms it employs for detecting unusual activities or intrusions. Over the years, a wide range of theft detection algorithms have been developed, leveraging machine learning, neural networks, and other computational techniques to improve accuracy and reduce false alarms. Among these, dynamic neural networks and ensemble methods like XGBoost have shown significant promise due to their ability to process large amounts of data and adapt to changing conditions in real-time.

This review paper aims to provide a comprehensive analysis of the various theft detection algorithms used in smart security systems. By evaluating their strengths, weaknesses, and areas for improvement, we can better understand the current state of the field and identify opportunities for future research and development. The ultimate goal is to enhance the effectiveness of smart security systems in protecting assets and ensuring safety in both residential and commercial settings.field.

II. LITERATURE SURVEY

Praveen Kallukalam Sebastian et.al (2023) Traditional analog and digital meters are being substantially replaced with technological advances and the Internet of Things (IoT) introduction. The smart meter is highly preferred for accessing real-time consumption, tariff calculation, and remote system control. These smart meters also prevent the majority from bypassing theft. Despite its intelligence, it cannot be 100% secure. An error in the readings can be caused by hacking or damage to meter components making the utility companies suffer significant losses. Based on past and future energy consumption data predictions on the consumer side, various methods are used in the proposed work to identify theft or anomalies in smart meter readings. Forecast-based detection proved to be the most effective and accurate method. The primary and secondary decision models, which employ a variety of statical analyses to identify system anomalies, serve as the foundation for the energy consumption that follows the forecasting. Past 24-h data is needed for forecasting, which is passed through different statical calculations such as RMSE, simple moving average, and Absolute Percentage Error to conclude detecting the normal values. Long short-term memory gives high accuracy of 97% for forecasting and detecting abnormalities[1].

Weixian Li et al (2019) studies on In the modern smart home, smart meters, and Internet of Things (IoT) have been massively deployed to replace traditional analogue meters. It digitalises the data collection and the meter readings. The data can be wirelessly transmitted that significantly reduces manual works. However, the community of smart home network is vulnerable to energy theft. Such attacks cannot be effectively detected since the existing techniques require certain devices to be installed to work. This imposes a challenge for energy theft detection systems to be implemented despite the lack of energy monitoring devices. This paper develops an energy detection system called smart energy theft system (SETS) based on machine learning and statistical models. There are three stages of decision-making modules, the first stage is the prediction model which uses multimodel forecasting system. This system integrates various machine learning models into a single forecast system for predicting the power consumption. The second stage is the primary decision making model that uses simple moving average (SMA) for filtering abnormally. The third stage is the secondary decision making model that makes the final stage of the decision on energy theft. The simulation results demonstrate that the proposed system can successfully detect 99.96% accuracy that enhances the security of the IoT-based smart home[2].

Mahmoud Nabil et al (2019) studies on Advanced metering infrastructure (AMI) is the primary step to establish a modern smart grid. AMI enables a flexible two-way communication between smart meters and utility company for monitoring and billing purposes. However, AMI suffers from the deceptive behavior of malicious consumers who report false electricity usage in order to reduce their bills, which is known as electricity theft cyber-attacks. In this chapter, we present deep learning-based detectors that can efficiently thwart electricity theft cyber-attacks in smart grid AMI networks. First, we present a customer-specific detector based on a deep feed-forward and recurrent neural networks (RNN). Then, we develop generalized electricity theft detectors that are more robust against contamination attacks compared with customer-specific detectors. In all detectors, optimization of hyperparameters is investigated to improve the performance of the developed detectors. In particular, the hyperparameters of the detectors are optimized via sequential, random, and genetic optimization-based grid search approaches. Extensive test studies are carried out against real energy consumption data to investigate all detectors performance. Also, the performance of the developed deep learning-based detectors is compared with a shallow machine learning approach and a superior performance is observed for the deep learning-based detectors[3].

Nadeem Javaid et al (2021) studies on The bi-directional flow of energy and information in the smart grid makes it possible to record and analyze the electricity consumption profiles of consumers. Because of the increasing rate of inflation over the past few years, people started looking for means to use electricity illegally, termed as electricity theft. Many

data analytics techniques are proposed in the literature for electricity theft detection (ETD). These techniques help in the detection of suspected illegal consumers. However, the existing approaches have a low ETD rate either due to improper handling of the imbalanced class problem in a dataset or the selection of inappropriate classifier. In this paper, a robust big data analytics technique is proposed to resolve the aforementioned concerns. Firstly, adaptive synthesis (ADASYN) is applied to handle the imbalanced class problem of data. Secondly convolutional neural network (CNN) and long-short term memory (LSTM) integrated deep siamese network (DSN) are proposed to discriminate the features of both honest and fraudulent consumers. Specifically, the task of feature extraction from weekly energy consumption profiles is handed over to the CNN module while the LSTM module performs the sequence learning. Finally, the DSN contemplates on the shared features provided by the CNN-LSTM and applies final judgment. The data analytics is performed on different train–test ratios of the real-time smart meters' data. The simulation results validate the proposed model's effectiveness in terms of high area under the curve, Score, precision and recall[4].

Zhongtao Chen etal (2020) studies on electricity theft causes significant harm to social and economic development. In the past few years, it has attracted much attention that electricity theft detection based on electricity consumption data can help to solve this problem. A major challenge is that there are no explicit features in electricity consumption records. However, the existing machine learning-based detection methods mainly suffer from the following two disadvantages. (1) Handcrafted features and shallow-architecture classifiers have poor detection accuracy. (2) Most methods consider electricity consumption as static and cannot capture both the internal time-series natures and external influence factors well. To overcome the above shortcomings, we propose a novel method called Electricity Theft Detection using Deep Bidirectional Recurrent Neural Network (ETD-DBRNN), which can capture the internal characteristics and the external correlation by learning the electricity consumption records and influence factors representation. Experiments on real-world datasets validate the effectiveness of our method[5].

III. METHODOLOGY

In this review, we conducted a thorough examination of theft detection algorithms used in smart security systems by analyzing existing literature and evaluating various approaches based on their performance metrics, such as accuracy, precision, recall, and F1-score. We focused on dynamic neural networks and machine learning methods, particularly XGBoost, to understand their application in real-time theft detection. The analysis involved comparing the algorithms across different datasets, examining their ability to identify theft events under varying conditions, and assessing their adaptability to changes in the environment. Additionally, we considered the computational complexity, scalability, and integration capabilities of these algorithms within smart security systems, ensuring a comprehensive evaluation of their practical utility and effectiveness.

IV. CONCLUSION

This review has provided a comprehensive analysis of various theft detection algorithms used in smart security systems, with a particular focus on dynamic neural networks and machine learning approaches like XGBoost. The evaluation of these algorithms revealed that while many exhibit high accuracy and reliability in detecting theft, their performance varies significantly depending on factors such as dataset characteristics, environmental conditions, and system integration. The XGBoost method, in particular, demonstrated robust performance across multiple metrics, making it a promising choice for real-time theft detection in smart security environments. However, challenges remain, including the need for improved accuracy in certain classes, scalability issues, and the integration of these algorithms into existing security frameworks. Future research should aim to address these challenges by developing more adaptable and efficient algorithms that can better handle diverse and dynamic scenarios within smart security systems. This will further enhance the effectiveness of theft detection and contribute to the advancement of intelligent security technologies..

REFRENCES

[1] Ramanpreet Kaur,, Duˇsan Gabrijelˇciˇc , Tomaˇz Klobuˇcar "Artificial intelligence for cybersecurity: Literature review and future research directions " Information Fusion Volume 97 , September 2023.

[2]. Shubhodip Sasmal "Preventing Card Fraud and Scam Using Artificial Intelligence " Criminal Law December 2021 DOI:10.55083/irjeas.2021.v09i04010

[3]. Waleed Hilal, S. Andrew Gadsden, John Yawney "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances" Expert Systems with Applications Volume 193, 1 May 2022.

[4]. Safdar Ali Abro, Lyu Guang Hua, Javed Ahmed Laghari, Muhammad Akram, Bhayo, and Abdul Aziz Manon "Machine learning based electricity theft detection using support vector machines " IJECE 14(02):1240~1250 2024.

[5]. Rahul Kumar Jha "Energy Theft Detection using Unsupervised Learning" November 2023 DOI:10.13140/RG.2.2.25576.65280

[6]. Rahul Chauhan, Kamal Kumar Ghanshala, R.C Joshi "Convolutional Neural Network (CNN) for Image Detection and Recognition " ICSCCC 2018 DOI:10.1109/ICSCCC.2018.8703316

[7]. Muhammad Ishfaque, Qianwei Dai, Nuhman ul Haq, Khanzaib Jadoon , Syed Muzyan Shahzad and Hammad Tariq Janjuhah " Use of Recurrent Neural Network with Long Short-Term Memory for Seepage Prediction at Tarbela Dam, KP, Pakistan" Energies 2022, 15(9), 3123; https://doi.org/10.3390/en15093123

[8]. Chihang Yang, Hao Zhang, Yang Gao " Analysis of a neural-network-based adaptive controller for deep-space formation flying " Advances in Space Research Volume 68, Issue 1, 1 July 2021, Pages 54-70

[9]. Ravi Raj & Andrzej Kos " An improved human activity recognition technique based on convolutional neural network" Nature Scientific Reports volume 13, Article number: 22581 (2023).

[10]. Lotfallahtabrizi, Parisa "A Novel Mobile Host Intrusion Detection Using Neural Networks " University of Regina 2018 https://hdl.handle.net/10294/8527

[11]. Adesh Kumar and Vijay Maheshawari "Analysis of Dynamic Intelligent NetworkSecurity System " International Journal of New Trends in Electronics and Communication (IJNTEC) Vol.1, Issue. 2, Sep. 2013 12. Pooja Br, Rajkumar N " Real-Time Intelligent Video Surveillance System using Recurrent Neural Network" Procedia Computer Science Volume 235, 2024, Pages 1522-1531

[12]. Ann Nosseir , Khaled Nagati and Islam Taj-Eddin " Intelligent Word-Based Spam Filter Detection Using Multi-Neural Networks " IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 1, March 2013

[13]. Alom, Md Zahangir, VenkataRamesh Bontupalli, and Tarek M. Taha. "Intrusion detection using deep belief networks." 2015 National Aerospace and Electronics Conference (NAECON). IEEE, 2015. Doi: 10.1109/NAECON.2015.7443094. [Access 27.04.2021].

[14.] Alazab, Mamoun, and MingJian Tang, eds. Deep learning applications for cyber security. Springer, 2019. https://doi.org/10.1007/978-3-030-13057-2_5. [Access 28.04.2021].

[15]. Kim, Jihyun, et al. "Long short-term memory recurrent neural network classifier for intrusion detection." 2016 International Conference on Platform Technology and Service (PlatCon). IEEE, 2016. Doi: 10.1109/PlatCon.2016.7456805. [Access 28.04.2021].

[16]. Kasongo, Sydney Mambwe, and Yanxia Sun. "A deep learning method with filterbased feature engineering for wireless intrusion detection system." IEEE Access 7 (2019): 38597-38607. Doi: 10.1109/ACCESS.2019.2905633. [Access 28.04.2021].

[17]. Naseer, Sheraz, et al. "Enhanced network anomaly detection based on deep neural networks." IEEE access 6 (2018): 48231-48246. Doi: 10.1109/ACCESS.2018.2863036. [Accessed 28.04.2021].

[18]. Gaur, Vimal, and Rajneesh Kumar. "Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices." Arabian Journal for Science and Engineering 47, no. 2 (2022): 1353-1374.

[19]. Pajila, P. J., E. Golden Julie, and Y. Harold Robinson. "FBDR-Fuzzy based DDoS attack

Detection and Recovery mechanism for wireless sensor networks." Wireless Personal Communications 122, no. 4 (2022): 3053-3083.

[20]. Banita lebi Dehkordi, Afsaneh, Mohammad Reza Soltanaghaei, and Farsad Zamani Boroujeni. "The DDoS attacks detection through machine learning and statistical methods in SDN." The Journal of Supercomputing 77, no. 3 (2021): 2383-2415.

[21]. Ahuja, Nisha, Gaurav Singal, and Debajyoti Mukhopadhyay. "DLSDN: Deep learning for DDOS attack detection in software defined networking." In 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), pp. 683-688. IEEE, 2021.