IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 15, May 2023

Impact of Machine Learning on Electricity Theft Detection

Prof. Pankaj Phadtare[1], Priti Chavan[2], Jay Kadam[3], Rugved Shinde[4], Velankanni Yadavar[5]

Department of Computer Engineering[1,2,3,4,5]

Trinity College of Engineering, Pune, India

Abstract: *The principal source of electrical power loss that has a substantial impact on both the quantity and quality of electrical power is electricity theft. However, the approaches currently in use for detecting this theft-related criminal activity are varied and complex since it is difficult to extract useful information from time-series data due to the uneven nature of the dataset. This research develops a novel approach for detecting electricity theft by combining three algorithms into a pipeline. The suggested approach first balances the dataset using the synthetic minority oversampling technique (SMOTE), then integrates kernel function and principal component analysis (KPCA) to extract features from highly dimensional time-series data, and uses support vector machines (SVM) to classify the data. Additionally, the effectiveness of the system.*

Keywords: ESP826612E, ATmega328, Thingsspeak IOT, Energy Meter, Display.

REFERENCES

[1]. J. Nagi, K. Yap, S. Tiong, S. Ahmed, and M. Mohamad, “Nontechnical loss detection for metered customers in power utility using support vector machines,” IEEE Transactions on Power Delivery, vol. 25, no. 2, pp. 1162–1171, 2010, cited By 104.

[2]. S. McLaughlin, D. Podkuiko, and P. McDaniel, “Energy theft in the advanced metering infrastructure,” Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 6027 LNCS, pp. 176–187, 2010, cited By 99.

[3]. G. Tsekouras, N. Hatziargyriou, and E. Dialynas, “Twostage pattern recognition of load curves for classification of electricity customers,” IEEE Transactions on Power Systems, vol. 22, no. 3, pp. 1120–1128, 2007, cited By 122. [Online].

[4]. Y. Zhang, W. Chen, and J. Black, “Anomaly detection in premise energy consumption data,” 2011, cited By 12. [Online].

[5]. S. Dua and X. Du, Data Mining and Machine Learning in Cybersecurity, 1st ed. Boston, MA, USA: Auerbach Publications, 2011.

[6]. V. Barnett and T. Lewis, Outliers in Statistical Data, ser. Wiley Series in Probability Statistics. Wiley, 1994. [Online].

[7]. Available: https://books.google.com.pr/books?id=B44QAQAAIAAJ

[8]. N. Billor, A. Hadi, and P. Velleman, “Bacon: Blocked adaptive computationally efficient outlier nominators,” Computational Statistics and Data Analysis, vol. 34, no. 3, pp. 279–298, 2000, cited By 154.

[9]. E. Eskin, “Anomaly detection over noisy data using learned probability distributions,” in Proceedings of the Seventeenth International Conference on Machine Learning, ser. ICML ’00. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2000, pp. 255–262.

[10]. E. M. Knorr and R. T. Ng, “Algorithms for mining distance-based outliers in large datasets,” in Proceedings of the 24rd International Conference on Very Large Data Bases, ser. VLDB ’98. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1998, pp. 392–403.

[11]. C. Aggarwal and P. Yu, “Outlier detection for high dimensional data,” 2001, pp. 37–46, cited By 433