*Detecting and Predicting Electricity Theft using*

*Machine Learning Algorithms*

Kawala Steven

X15018121

[X15018121@student.ncirl.ie](mailto:X15018121@student.ncirl.ie)

# **ABSTRCT**

Of the issue related with non-specialized irregularities in electricity usages, different strategies have been put in place for effective administration of non-specialized peculiarities in the electricity industry. The effective and best strategy implemented so far to diminish non-specialized peculiarities and revenue losses is the utilization of Smart advanced utility meters. This strategy makes deceitful exercises increasingly difficult, and it is simple to identify when such deceitful exercise happens. However, this strategy is not extensively utilized in most developing nations like Malawi because of the cost associated with the procurement and installation of the smart meters. This research paper looks at how well the proposed AI cost saving approach be utilized to identify and anticipate non-specialized oddities. The research proposes the use of; Random Forest, SVM, Naïve Bayes and Decision Tree models. These models will be implemented on local area power utilization, covering a year time frame verifiable data, to improve constant precision on the recognition of nontechnical inconsistencies. The models will distinguish and anticipate malevolent power utilization in real-time and chronicled data with anomalous utilization patterns will be associated with electricity theft. From other research, SVM method has been studied successfully in problem solving of anticipating and identify power theft on domestic level, despite showing weakness of limited capacity which has prevented the method from being used to solve other detection problems. Overall performance of SVM showed phenomenal results, in comparison with the other techniques. SVM performed well as a standalone technique as well as a hybrid with other techniques.

INTRODUCTION

Power extortion is a worldwide issue and it is costing utility companies a great deal of cash in revenue loss [17]. For the most part, the theft of power is related with, illegal electrical link reroutes and meter altering. The power theft techniques can be subdivided into under voltage and under current for example: destroying the seal of energy meter, open voltage hook of terminal in junction box, violated wire connections and even looping short electric current, making the electric energy meter shift slowly. Bypass across the meter, making less electric current pass through the meter for measurement. The power theft consequences, aside from income and conservative misfortune can likewise bring safety issue worries to the public for instance, causing electrical fire. Even though, in the reason for power theft catastrophes occur yet the fundamental destinations for the act is not to cause fire but the aggressors need to pay not exactly the standard expense of their power utilization, causing revenue loss for the utility companies. Nontechnical losses (NTLs) starting these power thefts are the most significant worries of any electricity company [4]. As an example, [2], pointed out that the USA alone losses $4.5 billion consistently and utility companies overall lose a gauge of more than 20 billion every year in revenue because of power theft. In further research, India reported $16.2 billion loss every year because of power theft and the USA uncovered $6 billion per year economical loss because of power theft [3]. This is one of the fundamental reasons why this domain area remains a research domain globally to save the utility companies from revenue loss. These losses affect utility companies in the way quality of supply ins maintained, increases electricity generation load and implementation of electricity tariff on sincere customers.

Generally power companies in most developing nations, use field auditors to explore the pernicious use of electricity at domestic unit level. This is dull and increases overhead expense of the company. The author sees a gap in the examination of power theft in most African nations especially Malawi, where field monitors are conveyed to explore the theft as opposed to utilizing a greater amount of AI. To address this exploration gap, this research paper proposes a relative investigation for identifying non-specialized irregularities utilizing diverse AI calculations, for example, Random Forest, SVM, Naïve Bayes and Decision Tree models on residential area electricity consumption that will improve continuous precision on the identification of a nontechnical inconsistency. Even though these recognition strategies give off an impression of being inventive, a few critics have said that there is yet a requirement for more research to be accomplished for the exhibition of the systems to be for all intents and purposes palatable. These contributory contentions make this space territory more fascinating for additional investigation. The aftereffects of this examination will propose a model that can be utilized to lessen nontechnical noxious electrical burden oddity which incorporate theft, and wellbeing issues relating to illegal connections of power supply. The general advantage of the success of using the proposed techniques will be the commitment that will be brought to the national economy.

For example, in most developing countries, reliable power supply attracts foreign businesses to invest in the country thereby creating employment and contributing to the GDP of the country Think about the impact of all the revenue being lost because of this malevolent exercise if that revenue was siphoned back into the national economy? The impact will be noticeable. To this end, the examination will be created utilizing a dataset sample covering a year time span chronicled data, which may have or never had vindictive exercises. The model will screen any varieties from the standard in client utilization examples to distinguish suspicious special cases. At that point a suspicion will be made on the chronicled data with irregular utilization patterns as having fraudulent activities. A. Research Question How well can AI calculations be utilized to identify and anticipate power theft? As per [5], there are various kinds of power theft that the exploration question can base on: "Physical Attacks, Cyber Attacks and Data Attacks", however the examination focuses on the physical and data attacks, where unexpected changes show up in customer load profiles, demonstrating fake exercises. The exploration question proposed is picked dependent on what [5] previously talked about in his literature and further referenced by [3]as a region for additional examination. B. Research Objective The goal of the exploration endeavours to respond to the examination question above in two parts: •To build up a model that can distinguish and anticipate malevolent power utilization continuously. •Use AI calculations (Random Forest, SVM, Naïve Bayes and Decision Tree) on local area power utilization to improve ongoing precision on discovery of nontechnical peculiarity. The outcomes from the model would then be able to frame a reason for the forensic investigators and auditors to assemble proof to bring to courtroom for execution of the culprits.

**ARTICLES TO EXPLORE**

[1] K. Siah Yap, S. Tiong, J. Nagi, J. S. P. Koh and F. Nagi, Comparison of Supervised Learning Techniques for Non-Technical Loss Detection in Power Utility, 2012.

[2] S. Li, Y. Han, X. Yao, S. Yingchen, J. Wang and Q. Zhao, "Electricity Theft Detection in Power Grids with Deep Learning and Random Forests", Journal of Electrical and Computer Engineering, vol. 2019, pp. 1-12, 2019. Available: 10.1155/2019/4136874.

[3] S. Singh, R. Bose and A. Joshi, "Energy theft detection for AMI using principal component analysis based reconstructed data", IET Cyber-Physical Systems: Theory & Applications, vol. 4, no. 2, pp. 179- 185, 2019. Available: 10.1049/iet-cps.2018.5050.

[4] A. Nizar, Z. Dong and Y. Wang, "Power Utility Nontechnical Loss Analysis with Extreme Learning Machine Method", IEEE Transactions on Power Systems, vol. 23, no. 3, pp. 946-955, 2008. Available: 10.1109/tpwrs.2008.926431.

[5] P. Jokar, N. Arianpoo and V. Leung, "Electricity Theft Detection in AMI Using Customers’ Consumption Patterns", IEEE Transactions on Smart Grid, vol. 7, no. 1, pp. 216-226, 2016. Available: 10.1109/tsg.2015.2425222.

[6] X. Wang and S. Ahn, "Real-time prediction and anomaly detection of electrical load in a residential community", Applied Energy, vol. 259, p. 114145, 2020. Available: 10.1016/j.apenergy.2019.114145.

[7] S. Li, Y. Han, X. Yao, S. Yingchen, J. Wang and Q. Zhao, "Electricity Theft Detection in Power Grids with Deep Learning and Random Forests", Journal of Electrical and Computer Engineering, vol. 2019, pp. 1-12, 2019. Available: 10.1155/2019/4136874.

[8] G. Dedene, S. Viaene and R. Derrig, A Case Study of Applying Boosting Naive Bayes to Claim Fraud Diagnosis, 2004. [Accessed 6 March 2020].

[9] M. Nabil, M. Ismail, M. Mahmoud, M. Shahin, K. Qaraqe and E. Serpedin, Deep Recurrent Electricity Theft Detection in AMI Networks with Random Tuning of Hyper-parameters, 2018. [Accessed 8 April 2020].

[10] J. Nagi, A. Mohammad, K. Yap, S. Tiong and S. Ahmed, Non-Technical Loss Analysis for Detection of Electricity Theft using Support Vector Machines, 2008. [Accessed 8 April 2020].

[11] Briseño, H. and Rojas, O., 2020. FACTORS ASSOCIATED WITH ELECTRICITY THEFT IN MEXICO. *International Journal of Energy Economics and Policy*, 10(3), pp.250-254.