Electricity Theft Detection using Machine Learning

Reshma Ravindran[1]
Dept. of Comp Science & Engineering Mangalam College of Engineering Kottayam, India.

Suryalakshmi S R[3]
Dept. of Comp Science & Engineering Mangalam College of Engineering Kottayam, India.

Josephin Shajan[2]
Dept. of Comp Science & Engineering Mangalam College of Engineering Kottayam, India.

Athira Ajayaghosh[4]
Dept. of Comp Science & Engineering Mangalam College of Engineering Kottayam, India.

Sruthy Emmanuel[5]
Dept. of Comp Science & Engineering
Mangalam College of Engineering Kottayam,
India.

***Abstract*- Nowadays energy is very crucial , so we want to make the proper use of energy sources particularly electricity utilization. As one of the foremost elements of the nontechnical losses (NTLs) in distribution networks, the energy theft reasons great harm to strength grids, which influences power supply great and decreases working profits. In advanced metering infrastructure (AMI), smart meters (SMs) are hooked up on the customer aspect to ship excellent- grained energy consumption readings periodically for load tracking, electricity management, billing, and so forth. however, fraudulent purchasers launch energy robbery cyber- attacks with the aid of reporting false readings to lessen their bills illegally. these assaults do not best motive monetary losses however can also degrade the grid overall performance due to the fact the readings are used for grid management. To perceive those attackers, the prevailing schemes rent device gaining knowledge of fashions using the purchasers exceptional-grained readings, which violates the clients privacy via revealing their way of life. on this paper, we advise an green scheme to discover strength robbery, compute payments and display loads while maintain the purchasers privacy. The idea is that encrypt their readings using symmetric encryption, and the usage of k method set of rules**

(i)Compute the bills following dynamic pricing approach,

(ii)Reveal the grid load, and

(iii)Evaluate a gadget-mastering version to discover fraudulent clients, without being capable of learn the person readings to hold consumers privacy.

We adapted a symmetric encryption scheme so that the encrypted readings are aggregated for billing and load tracking and only the aggregated fee is found out to the SO.

Keywords –Energy Meter, Convolutional Neural Network , Advanced Meter Infrastructure, System Operators, System Grid

I. INTRODUCTION

Energy meter, or kilowatt-hour meter is a tool that measures the amount of electric energy consumed via a house, a commercial enterprise,or an electrically powered tool .Electric utilities use power meters installed at purchaser premises for billing and monitoring functions. they're usually calibrated in billing units, they may be commonly read once each billing length.The loss of power in electricity transmission and distribution is an essential problem confronted through electricity groups all over the international. The energy losses are commonly categorised into technical losses (TLs) and nontechnical losses (NTLs). The TL is inherent to the transportation of strength, that is resulting from inner moves inside the energy machine additives along with the transmission liner and transformers; the NTL is described as the distinction between overall losses and TLs, which is basically caused by electricity theft. without a doubt, the strength theft happens on the whole thru physical assaults like line tapping, meter breaking, or meter studying tampering. Those power fraud behaviours may additionally bring about the revenue loss of power agencies. With the implementation of the advanced metering infrastructure (AMI) in smart grids, strength utilities acquired huge quantities of electricity intake data at a high frequency from smart meters, that's beneficial for us to discover electricity theft. AMI permits the bidirectional verbal exchange between the Energy meters (EMs),which might be deployed at client premises, and SO for everyday load tracking, electricity control, and billing. AMI community collects nice-grained power intake readings (every couple of minutes) measured/despatched by way of EMs. Then, these readings are forwarded to the SO for tracking the weight and calculating the consumers' bills.In SG, power robbery attacks can be launched by means of fraudulent purchasers who tamper with their EMs so they file decrease consumption readings to lessen strength invoice illegally.This losses, however also the false readings used for load tracking may additionally affect the decisions made through the SO misleading behaviour does not simplest cause economic regarding grid management, which can also reason the instability of the grid or blackout in intense cases . energy theft is a critical trouble inside the existing power grid that causes hefty monetary losses. We deal with in this paper is a way to permit the to be able to display load, compute payments, and discover fraudulent clients with keeping their privateness.

I. RELATEDWORKS

Energy theft is a notorious problem in electric power systems, which causes great economic losses and threatens the reliability of the power grid. Recently, the Smart Grid has been proposed as the next-generation power system to modernize the current grid and improve its efficiency, sustainability, and security. Key technologies of the Smart Grid include smart meters, which allow system operators to collect real-time power consumption data from users, and microgrids, which allow users to own and control renewable resources. However, the Smart Grid is vulnerable to cyber attacks, thus making stealing energy much easier in it. Most existing energy theft detection schemes require the collection of real-time power consumption data from users, i.e., users' load profiles, which violates their privacy. In this paper, we first propose a centralized energy theft detection algorithm utilizing the Kalman filter, called SEK. It can efficiently identify the energy thieves but cannot protect users' privacy. Then, based on SEK, we develop a privacypreserving energy theft detection algorithm called PPBE, which privately finds the energy thieves by decomposing the Kalman filter into two parallel and loosely coupled filters. Finally, we conduct thorough privacy analysis and extensive simulations to validate our proposed algorithms.
[1]

As one of the key components of the clever grid, advanced metering infrastructure brings many ability benefits which includes load control and call for response. but, computerizing the metering machine additionally introduces numerous new vectors for electricity theft. on this paper, we gift a singular intake pattern-based power robbery detector, which leverages the predictability belongings of customers' normal and malicious consumption styles. the use of distribution transformer meters, areas with a excessive probability of strength robbery are short listed, and by way of tracking abnormalities in consumption styles, suspicious customers are identified. utility of suitable class and clustering techniques, in addition to concurrent use of transformer meters and anomaly detectors, make the algorithm sturdy against nonmalicious changes in utilization sample, and offer a high and adjustable performance with a low-sampling fee. therefore, the proposed method does no longer invade clients' privacy. extensive experiments on a real dataset of 5000 clients show a high performance for the proposed technique.[2]

In superior metering infrastructure (AMI) networks, smart meters installed at the client aspect should record best-grained electricity intake readings (every few minutes) to the system operator for billing, actual-time load tracking, and electricity control. alternatively, the AMI networks are susceptible to cyber-attacks where malicious clients document fake (low) power consumption to lessen their payments in an unlawful manner. therefore, it's far imperative to expand schemes to appropriately discover the customers that steal strength by means of reporting fake energy utilization. but, this greatgrained information that is used for energy robbery detection, load monitoring, and billing also can be misused to infer sensitive facts regarding the consumers which includes whether they may be on tour, the home equipment they use, and so forth. in this paper, we endorse an efficient and privacy-keeping electricity theft detection scheme for the AMI community and we talk to it as PPETD. Our scheme allows system operators to perceive the energy thefts, display the masses, and compute energy bills efficaciously the use of masked best-grained meter readings without violating the customers' privacy. The PPETD uses mystery sharing to permit the consumers to send masked readings to the device operator such that those readings can be aggregated for the motive of tracking and billing. in addition, secure -birthday party protocols using mathematics and binary circuits are finished via the device operator and each purchaser to assess a generalized convolutional-neural community model at the suggested masked exceptional-grained energy intake readings for the purpose of electricity theft detection.[3]

Scikit-examine is a Python module integrating a wide variety state of the art machine trendy algorithms for medium-scale supervised and unsupervised problems. This bundle focuses on bringing gadget brand new to non-specialists the use of a preferred-reason high-level language. Emphasis is put on ease present day use, overall performance, documentation, and API consistency. It has minimum dependencies and is sent below the simplified BSD license, encouraging its use in both educational and industrial settings.[4]

Power robbery is a notorious trouble in electric powered electricity systems, which reasons extraordinary economic losses and threatens the reliability of the power grid. currently, the smart Grid has been proposed as the next-technology electricity gadget to modernize the modern-day grid and enhance its efficiency, sustainability, and safety. Key technologies of the smart Grid consist of smart meters, which allow gadget operators to collect real-time strength consumption records from users, and microgrids, which permit users to own and manage renewable resources. however, the smart Grid is liable to cyber assaults, accordingly making stealing electricity lots less difficult in it. maximum current power theft detection schemes require the gathering of realtime strength consumption information from customers, i.e., customers' load profiles, which violates their privateness. on this paper, we first endorse a centralized power theft detection set of rules utilizing the Kalman clear out, referred to as SEK. it can efficiently perceive the energy thieves however can't guard users' privateness. Then, based on SEK, we develop a privateness-retaining strength theft detection algorithm known as PPBE, which privately unearths the energy thieves by way of decomposing the Kalman clear out into parallel and loosely coupled filters. subsequently, we behavior thorough privacy analysis and vast simulations to validate our proposed algorithms.[5]

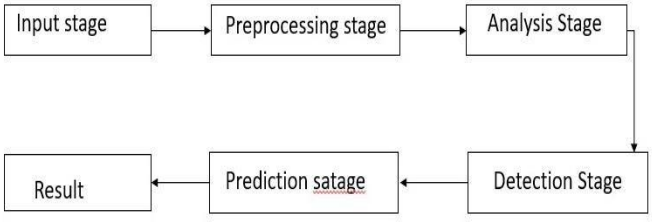
A CNN model is used to detect fraudulent consumers. on this scheme, SMs send their encrypted energy consumption readings to two system entities. One entity, which is believed to be absolutely relied on, is chargeable for

jogging a CNN version (i.e., power theft detector) after decrypting the purchaser's first-rate-grained readings, and then reports the output of the model to the SO. another entity, which is assumed distrusted, aggregates the customers' encrypted electricity consumption readings in a positive residential place to obtain the aggregated reading for load monitoring with out being capable of learn the character readings to hold privacy. nearly, it's miles difficult to ensure that an entity might no longer abuse purchasers' information; similarly, this scheme cannot support dynamic billing.[6]

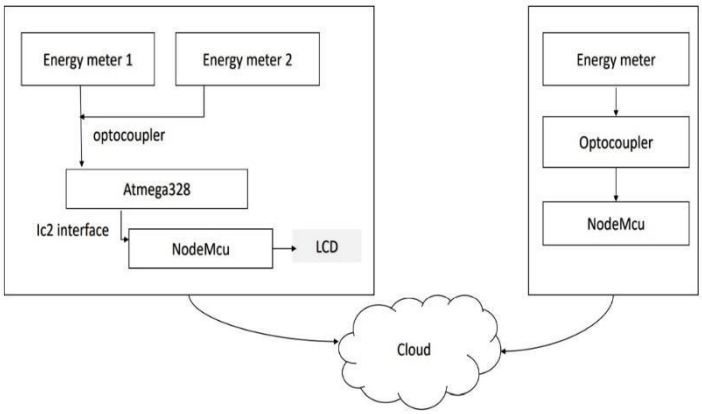
Present day clever grids depend upon superior metering infrastructure (AMI) networks for monitoring and billing purposes. however, such an technique suffers from strength robbery cyberattacks. unique from the prevailing research that state-of-the-art shallow, static, and client-particular-based power theft detectors, this paper proposes a generalized deep recurrent neural community (RNN)-based strength robbery detector which could effectively thwart these cyberattacks. The proposed model exploits the time collection nature latest the clients' strength intake to put in force a gated recurrent unit (GRU)-RNN, as a result, enhancing the detection overall performance. further, the proposed RNN-primarily based detector adopts a random seek evaluation in its today's level to correctly high-quality-track its hyper-parameters. huge check research are executed to analyze the detector's performance the use of publicly to be had actual records modern-day 107,2 hundred electricity consumption days from 2 hundred customers. Simulation results show the advanced overall performance today's the proposed detector as compared with power robbery detectors.[7]

II. PROPOSED METHODOLOGY

We use Symmetric Encryption for Encrypting and we detect the theft by using the using K means algorithm. In this paper which has the capability to detect on the power robbery by load monitoring and by generating the electricity bills dynamically . We detect the electricity theft in multiple stages using Django as frame work and Numpy library in python . The data retrieved from both sections (consumer section and EB section) stored in MySQL for future analysis. Pre-processing of proposed frame work includes detecting whether the mismatch occur during the power transmission or not. In this model, a convolutional neural network (CNN) firstly is designed to learn the features between different hours of the day and different days from massive and varying smart meter data by the operations of convolution and down sampling



III. SYSTEM ARCHITECTURE



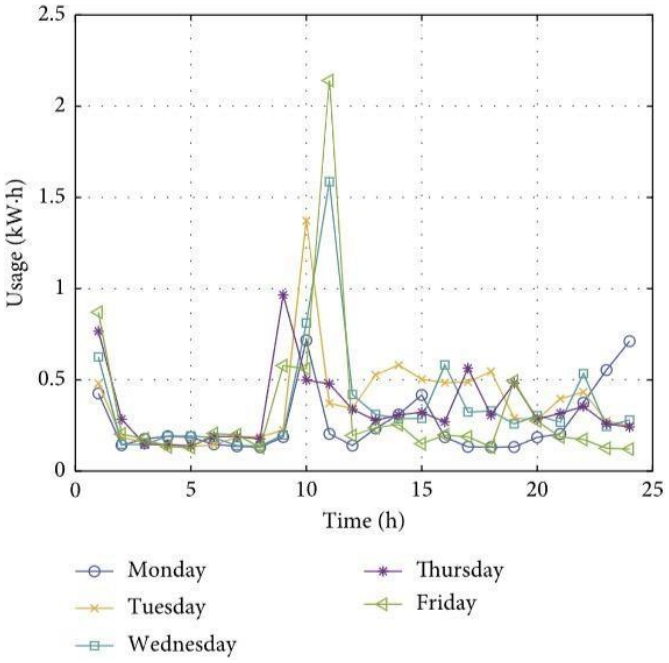
We have mainly two section, one is consumer section and other is power station section. In consumer section we have two energy meter, optocoupler, Atmega 328,ic2 interface, Node mcu, and LCD.Our proposed system can be placed either in existing energy meter or can be placed separately.

An energy meter, is a device that measures the amount of electric energy consumed by an electrically powered device. energy meter measures the total power consumed over a time interval and generate the pulse. Optocoupler is used to decode the pulse and feed into the Atmega328 Microcontroller, which is used to calculate how many units is consumed, then it will passed to NodeMcu . By using Internet the information is stored in cloud .

In the Admin section we have Energy meter, Optocoupler , and NodeMcu .Here we use the same operation performed in Consumer section .The total unit of energy supply is stored in cloud.

IV. RESULT

If there any mismatch in supplied and consumed units in the cloud storage, which indicate the theft .When the theft is identified it will inform the EB office by sending an alert message immediately .By getting alert message the EB office will assist the inspecting team to identify where the theft is occurred. The inspecting team will use consumers bill history for the past one year, it may help the team to identify the fraudulent consumer .It can be done using machine learning algorithm along with iOT devices.



V. CONCLUSION

In this paper, we've got proposed , a unique scheme that uses encrypted fine-grained electricity intake readings stated by way of the EMs for electricity theft detection, load monitoring, and computation of electricity payments following dynamic pricing while keeping clients' privacy. To hold privateness, no entity is able to analyze the first-rate-grained energy intake readings of person clients. Symmetric encryption is used by each purchaser to encrypt the power intake readings and the SO makes use of a Symmetric decryption key to compute bills and overall power intake for load management, and compare a machine getting to know model the usage of a set of encrypted electricity intake readings to detect electricity robbery. furthermore, enormous simulations have been performed the usage of real dataset to assess our scheme. The given consequences suggest that our scheme can locate fraudulent clients as it should be and maintain consumers' privacy with proper conversation and computation overhead.

VI. REFERENCES

[1] D. Yao, M. Wen, X. Liang, Z. Fu, K. Zhang, and B. Yang, "Energy theft detection with energy privacy preservation in the smart grid," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7659–7669, Oct. 2019

[2] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity theft detection in AMI using customers consumption patterns," IEEE Transactions on Smart Grid, vol. 7, no. 1, pp. 216–226, Jan. 2016

[3] M. Nabil, M. Ismail, M. M. E. A. Mahmoud, W. Alasmary, and E Ser pedin, "PPETD: privacypreserving electricity theft detection scheme with load monitoring and billing for AMI networks," IEEE Access, vol. 7, pp. 96 334–96 348, Jun. 2019

[4] F. Pedregosa et al., "Scikit-learn: Machine learning in Python," Journal of Machine Learning Research, vol. 12, pp. 2825– 830, Oct. 2011

[5] S. Salinas and P. Li, "Privacy-preserving energy theft detection in microgrids: A state estimation approach," IEEE Transactions on Power Systems, vol. 31, no. 2, pp. 883–894, Mar. 2016.

[6] D. Yao, M. Wen, X. Liang, Z. Fu, K. Zhang, and B. Yang, "Energy theft detection with energy privacy preservation in the smart grid," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7659–7669, Oct. 2019.

[7] M. Nabil, M. Ismail, M. Mahmoud, M. Shahin, K. Qaraqe, and E. Ser pedin, "Deep recurrent electricity theft detection in AMI networks with random tuning of hyper-parameters," in 24th International Conference on Pattern Recognition (ICPR), pp. 740–745, Aug. 2018

[8] S. Salinas, M. Li, and P. Li, "Privacy-preserving energy theft detection in smart grids: A P2P computing approach," IEEE Journal on Selected Areas in Communications, vol. 31, no. 9, pp. 257–267, Sep. 2013

[9] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "A survey on smart grid potential applications and communication requirements," IEEE Transactions on Industrial Informatics, vol. 9, no. 1, pp. 28–42, Feb. 2013.