Bulletin of Electrical Engineering and Informatics
Vol. 10, No. 1, February 2021, pp. 266~273
ISSN: 2302-9285, DOI: 10.11591/eei.v10i1.2026

A review of anomaly detection techniques in advanced metering infrastructure

Abbas M. Al-Ghaili[1], Zul-Azri Ibrahim[2], Syazwani Arissa Shah Hairi[3], Fiza Abdul Rahim[4], Hasventhran Baskaran[5], Noor Afiza Mohd Ariffin[6], and Hairoladenan Kasim[7]
[1,2,4]Institute of Informatics and Computing in Energy, Universiti Tenaga Nasional, Malaysia
[3,5,7]College of Computing & Informatics, Universiti Tenaga Nasional, Malaysia
[6]Department of Computer Science, Faculty of Computer Science & Information Technology, University Putra Malaysia**,** Malaysia

Article Info

Article history:

Received Dec 4, 2019
Revised Feb 28, 2020
Accepted May 4, 2020

Keywords:

AMI
Anomaly
Data manipulation
Smart meter

ABSTRACT

Advanced metering infrastructure (AMI) is a component of electrical networks that combines the energy and telecommunication infrastructure to collect, measure and analyze consumer energy consumptions. One of the main elements of AMI is a smart meter that used to manage electricity generation and distribution to end-user. The rapid implementation of AMI raises the need to deliver better maintenance performance and monitoring more efficiently while keeping consumers informed on their consumption habits. The convergence from analog to digital has made AMI tend to inherit the current vulnerabilities of digital devices that prone to cyber-attack, where attackers can manipulate the consumer energy consumption for their benefit. A huge amount of data generated in AMI allows attackers to manipulate the consumer energy consumption to their benefit once they manage to hack into the AMI environment. Anomalies detection is a technique can be used to identify any rare event such as data manipulation that happens in AMI based on the data collected from the smart meter. The purpose of this study is to review existing studies on anomalies techniques used to detect data manipulation in AMI and smart grid systems. Furthermore, several measurement methods and approaches used by existing studies will be addressed.

Corresponding Author:

Abbas M. Al-Ghaili,
Institute of Informatics and Computing in Energy,
Universiti Tenaga Nasional,
43000 Kajang, Selangor, Malaysia.
Email: abbas@uniten.edu.my

1. INTRODUCTION

In the energy sector, the utilization of electric meters was initially applied to industrial and commercial users because of the requirement to have more advanced data rates and progressively granular charging data demands [1]. The usage bit by bit extended to all end-user classes to accommodate a large number of customers. Automated meter reading (AMR) has been used to collect meter data by utilizing one-way communication. In recent years, advanced metering infrastructure (AMI) has been intensively built along with the evolution from the conventional electrical grid to the increasing growth of the smart grid. AMI will collect, calculate and analyze the consumer power consumption data and then transmit this information from a smart meter to a data collector center which then forwarded to a head-end system on the utility part. Figure 1 shows the common components of AMI, the transmission of data will start

from the end-user home appliance smart meter to the meter data management system (MDMS) where data analytics and measurement of the end-user consumption for billing and management purposed.

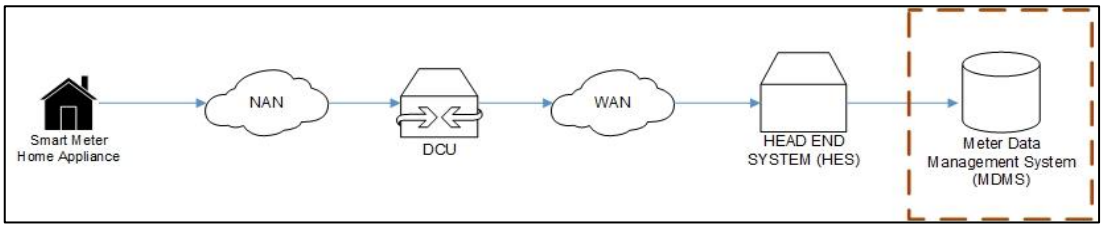

Figure 1. Advance metering infrastructure component

The rapid implementation of AMI rises the need to deliver better maintenance and monitoring more efficiently while keeping consumers informed on their consumption habits. The convergence from analog to the digital meter has made AMI tend to inherit the current vulnerabilities of digital devices that prone to cyber-attack, where attacker may gain benefit by manipulating consumers' energy consumption [2]. Telvent, a smart grid software company in 2012 announced that their network was hacked by a group of hackers that stole their data and infected their network with malware. Even this attack is considered a small scale attack but a larger scale attack can give a catastrophic impact that could trigger an electrical blackout and a total disruption to utility communication systems. In the current situation, according to [3], data produced by smart meter in AMI MDMS when tampered could lead to anomaly pattern which demands an anomaly detection techniques (ADTs) to detect them. As data produced in AMI is quite huge, finding the technique required to locate anomalies in huge amounts of data is just one of the several challenges that must be overcome in protecting the smart grid environment. In this study, a number of criteria have been applied to identify the relevant existing studies. One of these criteria is that the study must be between 2001 and 2019. Papers related to AMI and anomalies detection methods are the main and major focus in this review. The most recent published papers from conference proceedings and journals articles are cited in order to highlight only the latest applied cyber-attacks on energy sector-related smart meter data that deal with energy consumption for users. Further logical operators have been also applied to keywords during the searching process in several digital libraries. This paper is structured as follows: Section 2 will discuss the anomaly detection parameters. The discussion of selected studies is provided in section 3. Section 4 presents the conclusion of this work.

2. ANOMALY DETECTION PARAMETER

The past literature review has analyzed how the ADT is used in AMI and smart grid environment. There are several attacks were introduced to attack the dataset in the past literature paper. The ADT is used to detect the attack in the dataset. In order to evaluate the ADT, accuracy, computation time and trust parameters were developed.

2.1. Accuracy

Anomalies detection involves the process of detecting abnormal activities from a large volume of data, which in the AMI situation is the data supplied from the end-user smart meter to the utility provider power consumption database. In his report [4] stated that in Great Britain, the smart meter rolled out a project that began in 2011 and will be expected to end in 2020 to install 50 million new smart meters to 30 million homes and non-domestics sites. With the high volume of data collection in the smart meter raised the concerned on accuracy in detecting malicious intention to inject false data in the smart meter consumption accuracy is used to measure the performance of the different machine learning algorithms to be as accurate as possible.

As mention by [5] accuracy is an acceptable classified instance used in a model, while precision is the true positive (TP) instances between all instances that considered by a model as positive. The results of both false positive (FP) and false negative (FN) should be checked for fraud detection. In his work [5] has reported that utility companies in the United States (US) lost around 6 billion dollars per year because of energy theft activities. This leads to the demand for effective and accurate anomalies detection to prevent such attacks as the smart meter still can be considered as new technology. The pattern and data behavior still unpredictable which can cause high false-positive in anomalies detection. However, there are samples of

methods applied to concern the dynamical behavior of energy reads and measures retrieved from smart meter data e.g., [6] or to concern the load monitoring to reduce energy consumption utilizing smart meters [7]. Many techniques have been exploited to monitor the behavior of data or the load or specifically to detect anomalies e.g., Neural network or machine learning [8]. It is critical to review the previous works with the accuracy parameter used to measure the performance of different machine learning algorithms with ADT. An extensive research studies retrieved from literature will be reviewed and identified to measure the proportion of accurately grouped anomalies to all instances classified as anomalies.

2.2. Computation time

Time is a highly accurate parameter that can be used to measure the delay between the processing of actual data and tampered/intruded data. Time is instrumental to show an explicit view of anomalies when the fabricated data are compared with the actual data in a graphical view. The delay difference between the actual data and fabricated or attacked data can be a good indicator to identify anomalies in a system. Time-series forecasting is one of the efficient ways of detecting anomalies based on time. Any data which is associated with time is termed as time series. Time series data can be on a daily, hourly, monthly or yearly basis too [9]. Time series forecasting can solve typical time series forecasting problems such as demand estimation and sales forecasting and also prepare for future needs by estimating anomalies with the current data. Time plays a major part in anomaly detection for utility providers. Monitoring electrical consumption over fine-grained time intervals makes utility providers detect anomalies easily. The classification algorithm discussed in [5] detects different types of attack by having a time window for observation and detection. In another example, authors in [10] are using time periods or time intervals in their classification based technique to identify energy theft. This technique for energy-theft is defined as load profile classification where the power usage of customers is recorded over a period of time. By using time as a variable, any abnormal energy usage pattern can be distinguished from normal energy usage patterns. The use cases mentioned above show the reliability and usefulness of time in detecting anomalies.

2.3. Trust

Trusted computing group (TCG) has defined trusted computing as to improve the overall security, privacy, and trustworthiness of a variety of computing devices in a computing environment [10]. Trust is a metric involving nodes in a system, that referred to as the certainty of a node within the capacity, dependability, and consistency of other nodes. There are 2 types of trust which are direct trust and indirect trust [11]. Direct trust is dependent on viewing a node directly. Whereas indirect trust is based on reputation which monitoring of one node by another node on success rate for duration of time. The threat level is inversely proportional to the trust level. Lower trust level mean that threat level is high. This is why trust is a reliable parameter in anomaly detection. This concept is applied in [12] to justify the threat impact and to establish trust confidence on devices located in a Smart Grid.

Authors in [13] have used trust as a metric to evaluate the nodes' behaviors and reliability in a network. The nodes' trustworthiness is measured with values ranging from 1 to 0. Malicious behaviors are indicated by lower values. However, the handling of trust as an important parameter in certain systems has to be improved. Authors in [14] have mentioned that user trust in the deep neural network-based intrusion detection system (DNN-IDS) is imperative and high accuracy only is not enough. DNN-IDS's transparency hindering nature has to be reduced to be more communicative. This will eventually increase the level of user trust. Trust also plays an important role in anomaly detection for cloud providers. Cloud service providers (CSP) can select suitable cloud services observe the condition of CSP when performing service level agreement (SLA) by anomaly detection algorithm. At that point refreshes CSP trust values in real-time and dynamically alters the volume of request sent to the CSP according to their suitablility [15]. Trust is a very good indicator for detecting anomalies, and the above-mentioned use cases are a good example of demonstrating this.

3. RESULTS AND DISCUSSION

In [5], a new feature-engineering framework using the finite mixture model (FMM) clustering algorithm and genetic programming (GP) is proposed. The study created a practical model-agnostic feature-engineering framework for fraud-related NTL detection in AMIs. The irish CBT [16] dataset is used from more than 4000 households over 18 months and collected the energy consumption every 30 minutes. There are 6 type of attacks presented in this study: (1) all the sample multiple by the random chosen coefficient, (2) on-off attack where the consumption is set to zero during interval, (3) it multiple the consumptions by the irregular factor that changes after some time, (4) reports a variable in time arbitrary division of every day means utilization, (5) day by day mean utilization is always reported, and (6) the aggregate total of power utilization is accurately presented. In this work, the GP will process

the information sources of the time-series meter readings of clients and train the dataset and their soft group affiliations. Extra variable that can assist in clarifying any anomalies in user demand patterns will be produced that combine with the time-series meter reading users in the training dataset. The performance result for the accuracy is between 0.684 until 0.811 while the computation time is between 10.224 min until 82.113 min in detecting new types attacks such as zero day and theft events. Authors in [17] have utilized a random tuning of hyper-parameters in Tensorflow using programming language Python to detect electricity theft and have proposed a recurrent neural network (RNN)-based power theft detection to prevent cyber-attacks. This model utilized the time arrangement based on clients' power consumption to create a gated recurrent unit (GRU) which can learn customer power consumption patterns. Hence, this study was done using irish smart energy [18] real dataset of 5000 users from 2009 to 2010 which accumulated more than 536 days. The dataset contained customers meter readings for every 30 minutes. Each customer will produce in total 25,728 reports and the daily report for 200 customers with 107,200 days is recorded before they launch an attack. The result shows that the RNN-based detector has a better detection rate and a lower false acceptance rate. As such this technique only focus on the time-based pattern only.

Huang [19] suggested artificial neural networks (ANNs) detect energy theft. ANNs are a collection of neurons that associated with biologically propelled designs and arrange in layers architecture. In their work, the IEEE 13 Node Test Feeder [20] model system is utilized to identify any power theft. It includes 24 data sets that model the power stream of every bus in 24 hours, this could acquire users' utilization consistently. ANN can recognize power theft using three techniques: (1) separates the entire system into smaller section, which the power theft can be distinguished according to the plot, (2) splits the system into three stages for each stage of the system is treated as one research object, it utilized recursive Bayesian approach to detect load stage in distribution system and (3) like (1) consider the system as one research object. This work aims to prevent overfitting ANNs in the future with an exponential volume of train data and increase the efficiency in selecting training data from history but no specific calculation was presented. A better criterion to detect will be developed to identify dishonest users.

Authors in [21] have classified data falsification attacks into four types: additive, deductive, camouflage and conflict. In additive attack, there is a possibility which an adversary may tamper the smart meter data by adding up the values which may result in increased electricity bills which can damage customer confidence to power utility due to higher bills compare to other competitors. But if the utility companies participate in the demand response, these companies may experience losses in revenue due to the additive attack for unnecessary payment paid to the customer for caused peak shifts. While in deductive attack is referred to loss of income for electricity utility corporations. Cover-up or camouflage happens where the attacker will split the compromised meter into two groups with the same numbers that concurrently adopt an additive and deductive mode, correspondingly. The attack will stay undetected because of the overall input and output of the smart meters and the total demand and the whole usage of the power consumption may remain unchanged. Lastly conflict attack is a scenario that is reprensted as random attack of existence of additive and deductive attacks both in prevention of both attack from being detected. This attack is mixed type of attack with the unequal margin of falsification for each hidden attack type. In their study, Pecan Street [22] dataset is used to detect the data falsification attack using statistical technique. Even though the end result effiecienly shows an high detection rate of 98% with 7% of false positive but how the attack dataset generated was not presented and was based on intuitive of the reserachers.

Authors in [23] have suggested an artificial intelligence algorithm to detect electricity theft by using the machine learning feature space. This novel framework called electricity theft detection (ETD) which include a smart algorithm like k-nearest neighbour and ETD to identify fake buyer from the real customer using consumption behavior. ETD utilizes transformer meters and observes any anomalies in customer consumption patterns in providing a good solution to detect power theft in terms of cost efficiency while k-Nearest Neighbor makes the framework more robust with the retraining capability. The irish social science data archive center (ISSDA) [18] is used as the real-time dataset to validate their approach where the result of the accuracy for k-Nearest Neighbour is 88% while ETD is 93% which makes the ETD robust against any non-malicious changes in consumption pattern. Authors in [24] have proposed the entropy-based electricity theft detector (EBETD) approach to identify any energy theft activities. In their study, MATLAB is used to detect energy theft activities by tracing the dynamic behavior of the data consumed by the end-users. Entropy is used to measure the values between two random distributions when the attackers sends the tampered electricity consumption reading toward the control center. The entropy will compare the reading with the predefined threshold numbers that were preset using previous historical power consumption variation using entropy calculation. The control center will conclude that attack has been launch by the adversary. If when compared with each sample during the runtime at each time step produce an entropy value that is more than the predefined threshold value. The irish social science data archive center is used and 5 types of attack for energy theft were demonstrated:

a. A1, attacker changed the sequence number of the power consumption by replacing the first number with the last and submitted it to the control center
b. A2, adversary used the mean value from previous day and send it to control center
c. A3, the previous day's consumption of mean value of the
d. A4, multiplied all power consumption with random number selected
e. A5, multiplied using same random number on particular day

The result in their study shows that EBETD approach has detected the attack with high positive rate (DR). The detection attacks of A1 and A2 are 81.24 and 98.92% DR. While attacks A3, A4, and A5 are 77.03, 100, and 94.22% DR. Lastly, the trust level will achieve high level. As in attack A4, the DR is 100% and FPR is 23.13% when trust level is 90% so they set in their study as the trust level is 99%. Jokar [25] proposed ROC Curve tools to be used in order to detect energy theft by observing any anomalies in customer consumption trend. It shows a novel of consumption pattern-based energy theft detector (CPBETD), that used consistency instance of normal users and example from the pattern of malicious consumption. CPBETD is quite effective dealing with contamination attacks and non-malicious changes in consumption trends. The support vector machine (SVM) technique is used to predict the target value of the test data. The data vector is mapped to a higher dimensional space where information classes are progressively recognizable. At that point, an isolating hyper-plane with the most extreme edge to the nearest information focuses on each class is found. The irish smart energy trial [18] dataset is used in the study and its record half-hourly interval electricity usage reports for more than 5000 businesses and homes from 2009 to 2010. The overall performance of CPBETD algorithm used in this study, the accuracy obtains 95% while the detection rate 94% if the lower the value of Bayesian detection rate (BDR) while considering the tampering rate 0.72%.

Cody [26] in his work has proposed decision tree learning for distinguishing fake activity in fine-grained power consumption information. In their study, WEKA is used as a data mining tool to demonstrate a successful application of the proposed technique by using the root mean squared error [16] which is a statistical technique to calculate the variance between anticipated values and real values. M5P will present the normal user power consumption behavior which can predict future power consumption and trace any malicious activity. The outcomes exhibited the M5P decision tree learning algorithm can be used in tracing energy fraud. The dataset will be segmented into multiple branches according to the decision rules base on the input attributes and outputs. The irish social science data archive center [18] dataset is utilized in this work used to present the efficiency of their methodology. They aimed at improving the detection and prediction based on this model in their future study. The feature extraction algorithm can be considered to enhance the model in pre-processing methods with the ability to remove irrelevant and redundant features. Then correlation with other machine learning methodologies can be led in recognizing the positive and negative parts, for more robust fraud detection system.

In [27], ANNs have been recommended to identify fraud in energy consumption data. During the evaluation, they used WEKA as a machine learning tool and indicate fraudulent activities by detecting anomalies from each of the end user consumption behaviour. To calculated the variation between expected and real meter reading in the social science data archive center (ISSDA) dataset [18], root mean squared error (RMSE) [28] is used. A confusion matrix was then developed to measure the level of effectiveness of the energy consumption behaviour (ECB) in ANN, to indicate the true positives (TP), true negatives (TN), false positive (FP) and false negative (FN). In his approach, if TP with 93.75% reflect that the ratio of fraudulent activities classified accurately as data theft. While TN of 75.00% classified as normal data with normal activities. The FP of 25.00% is considered as fraud. Lastly, FN corresponds to the numbers of fraudulent activities that classified as normal behavior. TP highest value will indicates that the ECB's neural network manage to detect any anomalies of malicious behaviors in the dataset. While the FP of 25.00% shows some of the normal activity in NN was labeled as fraud. Although the result from experiment in this work was very positive but how the attack can changed the user dataset and what changes does attacker made is not presented.

The authors in [29] suggested a hybrid clustering technique to identify the vulnerability node cluster against the false data injection (FDI) attack. In their study, MATLAB is used to identify FDI attack on the AMI. The level of FDI is then classified based on the vulnerabilities poses by every node in AMI, the associated relationship of various nodes is obtained and clustered using enhanced constriction factor particle swarm optimization (CF-PSO) will categorize each node into the least, moderate and most vulnerable group. Using lengthy experiments utilizing two test systems, have shown that group with higher likelihood is more prone to undermining the operation of the system. The UCI machine learning repository [30] dataset is used which contains 58,000 user data including numerical attributes in a total of 9. The dataset is used to improves the clustering approach by evaluating the performance of the k-means and CF-PSO. They concluded in their work that verifying the same characteristics of nodes under FDI attacks is important in detecting this attack. In this work, they managed to present how a node in AMI can be more likely to be attacked in AMI. In their

future work, where the initial work is already under preparation, they suggested the protection and detection strategy in identifying the most vulnerable nodes in AMI. Summary of past literature for anomaly detection techniques (ADTs) in AMI shown in Table 1.

Table 1. Summary of past literature for ADTs in AMI

Publication						Parameter
Ref.	Focus	Dataset	Tools	Technique	Result	
[5]	A practical feature-engineering framework for electricity theft detection in smart grids	Irish CBT	AUC performance	FMM clustering algorithm	Accuracy 0.684 - 0.811. Computation time: 10.224 min - 82.113 min	Accuracy & Computation Time
[9]	Anomaly Detection with Time Series Forecasting	Data is a use case e.g., revenue, traffic) and it is at a day level with 12 metrics	Python, Keras & Auto Arima	Time series forecasting	Time series forecasting helps to prepare for future needs by estimating anomalies with the current data.	Computation Time
[17]	Electricity theft detection with the random tuning of hyperparameters	Irish Smart Energy	Tensorflow (Python)	NN	Detection rate - 93% False acceptance - 5%	Accuracy
[19]	Energy theft detection via ANN	Not Stated	Radial Distribution Test Feeders	ANNs	Future work	Accuracy
[12]	Behavioral Based Trust Metrics and the Smart Grid	Real-world cyber Security Gateway Syslog	MCM, BEA, and FCEA processors	Machine and statistical learning algorithms	The methods were found to be accurate with low false positive and negative rates	Trust
[14]	Improving User Trust on Deep NN based Intrusion Detection Systems	NSL-KDD	Layer-wise relevance propagation	Binary classification and multiclass classification	Binary classification (A ~97%; intrusions detected). Multi-class Classification (A ~94%; DoS attack detected at A ~98%)	Trust
[21]	Data falsification on smart meter consumption	Pecan	Not mentioned	Statistical	Detection rate - 98% False alarm rate - 7%	Accuracy & Trust
[23]	Detecting fraudulent consumer from the normal consumer based on the consumer's consumption pattern	Irish Social Science Data Archive	Feature Space	k-Nearest Neighbour ETD Algorithm	k-Nearest Neighbours: A ~ 88% ETD algorithm: A ~ 93%	Accuracy
[24]	Detecting energy theft using entropy	Irish Social Science Data Archive Center	MATLAB R2014b	Entropy- based detection	Detection rate: A1=81.24 A2=98.92 A3=77.03 A4=100 A5=94.22 Trust=99%	Accuracy & Trust T
[25]	Detecting energy theft by monitoring abnormalities in customer consumption patterns	Irish Smart Energy	ROC curve	Support Vector Machine	Financial loss with A ~95%. detection rate 94%; tampering rate 0.72%	Accuracy
[13]	Adaptive Threshold Selection for Trust-based Detection Systems	Network flows collected by a European Internet Service Provider (ISP	Beta probability density function & ROC Curve	Host-degree and port-degree experiments	The host degree's threshold for STATIC-TPR is 5 and Port-degree's threshold value is the same too. True Positive Rate (TPR) is above 70% over 14 days.	Trust
[26]	Fraud Detection in Consumer Energy Consumption	Irish Social Science Data Archive Center	WEKA (Java)	Statistical	Future work	Accuracy

Table 1. Summary of past literature for ADTs in AMI *(Continue)*

Publication						Parameter
Ref.	Focus	Dataset	Tools	Technique	Result	
[11]	Neighbor node trust-based intrusion detection system for WSN	recommendation database	MATLAB	Trust calculation of neighboring node	The average detection rate is 0.8 per 100 results.	Trust
[27]	Energy fraud detection in energy consumption data	Irish Social Science Data Archive Center	WEKA (Java)	ANNs	A: Fraud FP ~25.00%; True negative ~75.00% True positive ~93.75% FN ~6.25%	Accuracy
[29]	Identification of vulnerable node clusters against FDI attack	UCI Machine Learning Repository	MATLAB	Hybrid clustering technique	Future work	-
[10]	Energy-Theft Detection Issues for Advanced Metering Infrastructure in Smart Grid	Not stated	Not stated	Attack tree-based threat model and categorization of energy-theft	Current AMI energy-theft detection schemes might be classification-based, state estimation-based, or game theory-based.	Computation Time
[31]	Computational Complexity of Anomaly Detection Methods	DARPA1999	Not stated	Entropy-based Multidimensional Mahalanobis-distance Method (EMMM) and CSDM method of $\chi 2$ value using multi statistical variables	The total time complexity of the EMMM method is O(n) for the n total packets.	Computation Time

4. CONCLUSION AND FUTURE WORKS

Various potential security issues related to AMI have been identified and an actual threat scenario has been implemented confirming the vulnerability of AMI environments. Apparently, ADTs are going to face challenges and difficulties to combat such rapidly emerging new threats. It is essential to identify abnormal activities that can decrease the functional risks, unexpected downtime and to avoid unseen problems of the AMI related components. Thus, detection of anomalies mechanisms needs to be continuously upgraded and enhanced in order to increase the security level critical data in the AMI environment. In summary, it is important to have a detection mechanism in place to ensure that data transmission in the AMI infrastructure is secure and not easily manipulated. This review reveals the various suggestions and implementation of ADTs. In evaluating the techniques, most existing studies focused on producing accurate results. However, there are also a number of studies that focused on computation time and trust issues. MATLAB is found as a popular tool of choice for demonstration and evaluation purposes. This review may provide references in obtaining detailed information on various ADTs approaches established in the AMI environment. Further improvement of the new techniques and procedures is required to process the diverse data streams produced in the AMI environment in order to achieve an accurate detection rate.

ACKNOWLEDGMENT

The authors would like to thank the Ministry of Higher Education Malaysia (MoHE) and Universiti Tenaga Nasional (UNITEN) for funding this study under the Fundamental Research Grant Scheme (FRGS) of Grant No. FRGS/1/2017/ICT03/UNITEN/03/1.

REFERENCES

[1] Edison and A. MeterComittees, "Smart Meters and Smart Meter Systems: A Metering Industry Perspective," *An EEI-AEIC-UTC White Paper*, pp. 1-35, 2011.
[2] Z.-A. Ibrahim, F. A. Rahim, R. Ismail, and A. A. Bakar, "A Review of Big Data Digital Forensic Analysis in Advanced Metering Infrastructure," *Advanced Science Letters*, vol. 24, no. 3, pp. 1603-1607, 2018.
[3] G. Muruti, F. A. Rahim and Z. bin Ibrahim, "A Survey on Anomalies Detection Techniques and Measurement Methods," *2018 IEEE Conference on Application, Information and Network Security (AINS)*, Langkawi, Malaysia, pp. 81-86, 2018.

[4] Paul Bolton, Sarah Barber, "Energy Smart Meters," *House of Commons Library Briefing Paper*, no. 8119,pp. 1-26, Oct 2019.
[5] R. Razavi, A. Gharipour, M. Fleury, and I. J. Akpan, "A practical feature-engineering framework for electricity theft detection in smart grids," *Applied Energy*, vol. 238, pp. 481-494, March 2019.
[6] A. M. Al-Ghaili, H. Baskaran, Z. Ibrahim, F. A. Rahim and S. A. S. Hairi, "A Dynamical Behavior Measurement Algorithm for Smart Meter Data: An Analytical Study," *2019 IEEE Conference on Application, Information and Network Security (AINS)*, Pulau Pinang, Malaysia, pp. 66-70, 2019.
[7] K. Khalid, A. Mohamed, R. Mohamed, and H. Shareef, "Performance Comparison of Artificial Intelligence Techniques for Non-intrusive Electrical Load Monitoring," *Bulletin of Electrical Engineering and Informatics*, vol. 7, no. 2, pp. 143-152, 2018.
[8] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Effective and efficient network anomaly detection system using machine learning algorithm," *Bulletin of Electrical Engineering and Informatics*, vol. 8, no. 1, pp. 46-51, 2019.
[9] A. Krishnan. "Anomaly Detection with Time Series Forecasting," *M toward data science*, [Online]. Available: https://towardsdatascience.com/anomaly-detection-with-time-series-forecasting-c34c6d04b24a, 2019.
[10] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen and X. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," in *Tsinghua Science and Technology*, vol. 19, no. 2, pp. 105-120, April 2014.
[11] S. M. Sajjad, S. H. Bouk, and M. Yousaf, "Neighbor Node Trust based Intrusion Detection System for WSN," *Procedia Computer Science*, vol. 63, pp. 183-188, 2015.
[12] J. Obert, A. Chavez and J. Johnson, "Behavioral Based Trust Metrics and the Smart Grid," 2*018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, New York, NY, pp. 1490-1493, 2018.
[13] Y. Chae, N. Katenka and L. Dipippo, "Adaptive Threshold Selection for Trust-Based Detection Systems," *2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)*, Barcelona, pp. 281-287, 2016.
[14] K. Amarasinghe and M. Manic, "Improving User Trust on Deep Neural Networks Based Intrusion Detection Systems," *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, Washington, DC, pp. 3262-3268, 2018.
[15] Y. Jin and S. Min, "Stadam: A new SLA trust model based on anomaly detection and multi-cloud," *2016 First IEEE International Conference on Computer Communication and the Internet (ICCCI)*, Wuhan, pp. 396-399, 2016.
[16] G. Martin, "Electricity smart metering customer behaviour trials findings report, Technical report," *CER Commission for Energy REgulation*, pp. 1-146, 2011.
[17] 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 24th International Conference on Pattern Recognition (ICPR)*, Beijing, pp. 740-745, 2018.
[18] J. McBride, "What is the Irish Social Science Data Archive?," *Journal Irish Political Studies*, vol. 17, no. sup 1, pp. 1-3, 200.
[19] H. Huang, S. Liu and K. Davis, "Energy Theft Detection Via Artificial Neural Networks," *2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, Sarajevo, pp. 1-6, 2018.
[20] W. H. Kersting, "Radial distribution test feeders," in *IEEE Transactions on Power Systems*, vol. 6, no. 3, pp. 975-985, Aug 1991.
[21] S. Bhattacharjee, A. Thakur, S. Silvestri, and S. K. Das, "Statistical Security Incident Forensics against Data Falsification in Smart Grid Advanced Metering Infrastructure," *Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy*, Scottsdale, Arizona, USA, pp. 35-45, 2017.
[22] N. None, "Pecan Street Grid Demonstration Program. Final technology performance report,"; *Pecan Street Project*, Inc., Austin, TX (United States), 2015. [Online]. Available: https://www.osti.gov/servlets/purl/1172297.
[23] R. Sowndarya and P. Latha, "An Artificial Intelligent Algorithm for Electricity Theft Detection in AMI," *International Journal of Engineering Science and Computing*, vol. 7, no. 3, pp. 5222-5227, 2017.
[24] S. K. Singh, R. Bose and A. Joshi, "Entropy-based electricity theft detection in AMI network," in *IET Cyber-Physical Systems: Theory & Applications*, vol. 3, no. 2, pp. 99-105, 2018.
[25] P. Jokar, N. Arianpoo and V. C. M. Leung, "Electricity Theft Detection in AMI Using Customers' Consumption Patterns," in *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 216-226, Jan 2016.
[26] C. Cody, V. Ford and A. Siraj, "Decision Tree Learning for Fraud Detection in Consumer Energy Consumption," *2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA)*, Miami, FL, pp. 1175-1179, 2015.
[27] V. Ford, A. Siraj and W. Eberle, "Smart grid energy fraud detection using artificial neural networks," *2014 IEEE Symposium on Computational Intelligence Applications in Smart Grid (CIASG)*, Orlando, FL, pp. 1-6, 2014.
[28] M. P. Anderson, M. P. Anderson, William W. Woessner, and R. J. Hunt Eds, "Applied Groundwater Modeling: Simulation of Flow and Adjective Transport,". *San Diego: Academic Press*, 2015.
[29] A. Anwar, A. N. Mahmood, and Z. Tari, "Identification of vulnerable node clusters against false data injection attack in an AMI based Smart Grid," *Information Systems*, vol. 53, pp. 201-212, 2015.
[30] Anand Sarwate, "UCI Machine Learning Repository,"*An Ergodic Walk*, 2013.
[31] S. Oshima and T. Nakashima, "Computational Complexity of Anomaly Detection Methods," *2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications*, Victoria, BC, pp. 644-649, 2012.