Electricity theft detection by sources of threats for smart city planning

Abdulrahman Okino Otuze$^{1,2}$, Mohd Wazir Mustafa$^1$, Olutunji Obalowo Mohammed$^{1,2}$, Muhammad Salman Saeed$^3$, Nazmat Toyin Surajudeen-Bakinde$^2$, Sani Salisu$^{1,3}$

$^1$Department of Electrical Power Engineering, School of Electrical Engineering, Universiti Teknologi Malaysia, Johor Bahru, Malaysia
$^2$Department of Electrical and Electronics Engineering, Faculty of Engineering and Technology, University of Ilorin, Ilorin, Nigeria
$^3$Department of Electrical Power Engineering, Ahmadu Bello University, Zaria, Nigeria

E-mail: ooadulrahaman2@live.utm.my

Abstract: Smart city adoption and deployment has taken the centre stage worldwide with its realisation clearly hinged on energy efficiency, but its planning is threatened by the vulnerability of smart grids (SGs). Adversaries launch attacks with various motives, but the rampaging electricity theft menace is causing major concerns to SGs deployments and consequently, energy efficiency. Smart electricity meters deployments via the advanced metering infrastructure present promising solutions and even greater potential as it provides adequate data for analytical inferences for achieving proactive measures against various cyberattacks. This study suggests the sources of threats as the first step of such proactive measures of curbing electricity thefts. It provides a framework for monitoring, identifying and curbing the threats based on factors indicative of electricity thefts in a smart utility network. The proposed framework basically focuses on these symptoms of the identified threats indicative of possible electricity theft occurrence to decide on preventing thefts. This study gives a useful background to smart city planners in realising a more reliable, robust and secured energy management scheme required for a sustainable city.

1 Introduction

The adoption and implementation of smart cities (SCs) have drawn worldwide attention and effective energy management is key to achieving this feat [1]. Energy management relies much on optimal consumption of energy and appropriate bill payment as set by the utility companies. This is facilitated by the trend in ICT deployment which has modernised the power grid for a secured, highly reliable, self-healing, real-time demand response and highly efficient operations known as smart grid (SGs) [2, 3]. SGs involve intelligent integration, monitoring and control of all power systems operations to deliver a more technically stable, economically inclined, socially driven, efficient power supplies and services [3–5] basically employing internet of things (IOTs) by the incorporation of sensing devices, actuators, communication and network devices [1, 6–8] for a robust smart cities (SCs) planning.

SGs present digitalisation of power consumption and pricing scheme as well as control via the advanced metering infrastructure (AMI) offering the use of smart electricity meters (SEMs) at both customer ends and substations which enables two-way communication between the SEMs and utilities [2, 9–11] suitable for a smart utility network. The AMI helps in real-time transmission of consumption data, instantaneous pricing information and management by the use of control commands [9, 10, 12]. They measure the values of energy flow and communicate these data with utilities, customers and third parties (usually, the network and other service providers) as depicted in Fig. 1 [2, 13, 14].

Generally, the AMI systems consist of the SEM, customer gateway, communication network and a headend. The SEMs mainly record and communicate the energy-related information. Usually, they are configured to record and provide customer’s energy consumption and billing data at a specified interval of usually per minute. The customer gateway is the layer responsible for the communication link between the AMI network and customer systems and appliances. The AMI Communications Network provides the link for information flow between the SEM and the AMI headend. A key aspect of the communication network is the home area network (HAN) responsible for the real-time communication of the consumption data between each of the connected devices and the SEMs within a consumer’s premises. Hacking of the HAN could potentially lead to data manipulations and consequently, energy theft [15]. The AMI headend is the subsystem which manages the information flow between external systems, such as the meter data management system and the AMI network [16]. Fig. 1 shows each customer monitors the information communicated by the corresponding SEMs which are also made available to utilities and third parties through the AMI.

Although, greatly reduced by the introduction of SEMs, electricity thefts remain a major concern to the deployment of AMI as adversaries continue to explore the vulnerabilities [2, 17]. Electricity theft has become a worldwide phenomenon causing huge technical and economic losses to operators and governments. The implementation of the digital metering system via the AMI utilising cyber layers presents a relief to the risk of energy thefts but introduced new dimensions [18, 19] posing unique challenges on the detection of non-technical losses (NTLs), hence, requiring

Fig. 1 Simplified AMI architecture
robust techniques [2, 9] specifically, focusing on mode of attacks and has continued to garner momentum especially with SCs being widely deployed.

Various modes of attacks present symptoms, which can be studied to present an active model for a timely identification of threats for improved safety and availability. In this study, a deterministic framework for curbing energy theft based on the symptoms of identified sources of threats is proposed. The states of the parameters of the manifesting symptoms are then used to make decisions on the possibilities of occurrence of electricity thefts. The sources of threats rely on the different modes of electricity thefts via the SEMs and it’s a key study to the effective planning of smart cities.

The rest of this paper is arranged as follows: Section 2 discusses issues relating to electricity thefts and smart metering. In Section 3, smart city energy management scheme is briefly explained while some literature of related works is discussed in Section 4. Section 5 explores the security requirements of AMI and its sources of threats, the proposed framework for monitoring and clearing these threats with its illustrated modelling are summed up in Section 6 and Section 7 concludes the study.

2 Electricity thefts and smart metering

The losses in power systems network are mainly categorised into technical losses (TLs), comprising the power dissipated in power systems’ components (e.g. transmission and distribution lines, transformers, protective devices etc.) and NTLs, comprising of those losses not traceable to any technical components. TLs occur naturally and are often calculated based on the systems’ components and network parameters while the electricity thefts form the major lump of the NTLs [20, 21]. Hence, energy thefts are often used interchangeably with NTLs.

Electricity thefts are fuelled by psycho-social factors, socio-economic factors, poor government policies and implementation etc. [21, 22] and although comes with dare consequences, the rate of its perpetuation knows no bound and has; therefore, instilled fears which must be studied for effective SCs planning. Possible victims of electricity thefts include electrocution due to unsafe illegal connections, huge revenue losses, increased tariff regime, high subsidy payments by government to make the tariffs affordable, inability to meet load demand by installed capacity, overloading of generation units, reduced reliability in grid operations and sometimes, unfavourable load shedding as utilities tend to favour the areas where increased revenue is realised, damage to infrastructure, discouragement of private sectors involvements, huge tasks and high expenses involved in the attempt to curb the menace especially, in conventional power systems etc. [2, 3, 19, 20, 22–24].

In traditional systems, energy theft has generated tremendous concerns as many loopholes are explored to cause NTLs, some of which include unauthorised line tampering and diversions, mechanical manipulations of the meter, meter bypass (partial or complete), meter swapping, faulty meters, unauthorised tariff regime, billing irregularities, non-payment of bills, poor revenue collection techniques, bad debt concepts, corrupt practices with internal staff for deliberate lowering of bills, ineffective governance or accountability by the power sector, political instability, high levels of corruption [21, 25–27] etc. However, these have been massively curtailed by the introduction of SEMs in AMI.

Worldwide, 313 million SEMs were reported to have been installed as at 2013 and this figure is projected to be about 852 million by 2020 and 2023, respectively [10, 28]. The EU estimates that by 2020, 237 million SEMs would have been installed in a deal of about 90 of 400 SGs project launched across Europe [29]. The US, one of the largest markets had over 70 million SEMs reported installed as at 2016 out of which 88% were deployed to monitor household consumers [29]. The North American region is projected to increase its installation at an annual compound growth rate of 6.0% from 100.7 million to 142.8 million in 2018 and 2024, respectively, while the Asia-Pacific is projected to increase its base from 618.8 million to 975 million in 2018 and 2024, respectively [30].

Nonetheless, many power grids around the world are yet to significantly key in to adopt the AMI even though SG deployment has presented solutions to many existing issues in the traditional grid [10]. These include real-time monitoring, improved response of energy consumption usage and dynamic billings, enhanced revenue generation monitoring and management as outages and faults are easily detected and reported, improved security against tampering, remotely controlled and local reading ability, interoperability within the SGs network, device and energy status capture by non-intrusive monitoring, support for HANs, bi-directional metering, renewable energy generation and integration support, provision of adequate data used in processing and classifications for pattern identification and consequent decision support [2, 5, 6, 10, 11, 21, 23–34].

SEMs have also helped to eliminate the associated cost of on-site reading of conventional meters and bills payments, on-field monitoring of customers in case of thefts, disconnection of faulty consumers [21] etc., although, they are now themselves, the main target with some rising drawbacks as adversaries continue to explore the vulnerabilities through the AMI. These drawbacks include the possibility of breaching customers’ privacy, causing a denial of service (DoS) attack or false data injection (FDI) subjecting the system's availability to question as a result of its dependence on network service. Health issues as a result of electromagnetic radiations have also been raised [10, 24, 33, 35].

AMI attacks are mostly launched during communication of the data with utility to falsify recorded data solely aimed at causing billing malfunctioning [36, 37]. These threats often originate basically from three attackers, namely, customers, insiders and terrorists/static attackers with the main aim of corrupting the integrity of the system to cause DoSs or data injection aimed at committing frauds. The customer attackers also known as fraudulent or unethical customers are usually less sophisticated in their modes of attacks but represent highest probability of threats to the AMI [12].

Depending on the intent and sophistication of the attackers, NTLs in the AMI are caused by false data injection via smart meters, meter tampering (by removal of the seals), error in computation of TLs, unlawful tapping from the secondary voltage sides of the transformer, general cyber-related attacks which may affect the networks, buying and selling of illegal prepaid vouchers, questionable employees' integrity etc. [2, 19–21, 26, 36, 38–40].

Fig. 2 sums up the modes by which electricity thefts are committed via SEMs. The figure shows that mainly, thefts via SEMs are carried out from customer end, through the distribution feeder lines and via the utility. The utility here is viewed to comprise all service operations including those performed by third parties.

While SGs offer a more secure system, caution must be observed because a very little per cent (of say, 1–2%) energy theft could translate to huge financial losses [23] since huge investments are always involved. In developing countries, about 20–45% of the revenue is reportedly lost to electricity theft while the figure stands between 3.5 and 30% in developed nations [41]. In the United States alone, over $6 billion dollars are lost to energy theft while about $25 billion are reportedly lost, worldwide [2, 17, 21, 38].

Some governments even grant subsidies to enable utility companies to make up for the losses in revenue due to energy theft [17, 42]. For efficient SC planning, these losses must be eliminated or at least, controlled to within relatively very low values by monitoring and controlling the energy consumption and billings for desired energy management and efficiency.

3 Smart city energy management

Smart cities are planned to integrate the operations of every infrastructure and services such as supply of efficient and secured electricity delivery scheme, safe water supplies, well-coordinated health care delivery systems; various marketing structures and platforms; efficient manufacturing and all industrial processes; security systems and operations; well-organised education and research systems etc. With this massive thought of integration
hinging exclusively SGs [43]. As many as there are connected ‘things’ in the smart city, it is imperative to ensure its associated energy consumption and billings are coordinated, monitored, efficient and secured from energy theft menace. Technological and non-technological approaches are often employed in electricity theft detection with each of the approaches complementing each other. Although the technological approach is expected to lay a chart by which the non-technological approaches can be achieved [3]. In traditional systems, it is compulsory to carry out on-site inspections while in SGs, a proactive scheme is well articulated on the basis that SCs operate primarily based on IoTs and require a robust energy management scheme as depicted in Fig. 3. The figure shows that SC relies on energy efficiency just as energy efficiency defines how smart a city is.

While effective consumption and consequently, effective energy billings and collection are a key aspect, electricity theft stands a barrier. This necessitates the inclusion of the detection and correction scheme. Evidently, theft or related attacks on the AMI cause huge losses and militates against further investment plans [17] except with assurance based on adequate security provision, hence, necessitating efficient tracing of threats and detection techniques for curbing these menaces [4]. The energy management scheme presented in Fig. 3 is a key aspect of smart city planning and must be well articulated especially by capitalising on available data.

Fortunately, SEMs make a frequent sampling of data at shorter regular interval available for finer loss rate calculations applicable in theft detection to a very high precision [40, 44]. This data can then be analysed to determine its health status against every identified threat. Given the various threats to energy infrastructure, threat models are aimed at providing awareness on identifying vulnerabilities with adequate strategies of monitoring to curb the menace [41]. Many efforts have been reported in the existing literature and they give a solid background to how these threat models have been previously approached.

Therefore, a well-planned SC must consider energy efficiency and sustainability as key factors. This can be achieved by providing real-time monitoring of power consumption and billing data for the analysis of usage trends to help in anomaly detection for consequent actions to guarantee energy efficiency [45].

4 Related works

Generally, it is difficult to compute NTLs but are usually estimated based on the total energy supplied and its corresponding billings [20]. SEMs via the AMI make the analysis for several situational inferences possible by the storage of large energy data. This has led to the development and application of many techniques involving data mining, statistics and mathematics, Machine learning prediction and classification algorithms, rules and states based techniques, cryptography, information-theoretic security [18, 19, 31, 44] etc.

Electricity detections via the AMI are examined from three basic categories, viz, the state-based estimations, game-theoretic approach and classification- or prediction- based techniques. The state-based involve designing a device for a high monitoring and detection accuracy but with higher investment price while the game-theoretic approach is based on formulation of game theory based on certain defined rules between the utility and the thief although with low cost but failed to provide an optimal solution, whereas the classification- or prediction-based algorithms involve the aggregation of SEMs energy consumption data for analysis and inferences using robust data mining and machine learning techniques to train a classifier for load profiling or forecasting and detection of abnormal patterns [2, 37, 46–49]. Due to the problem of data imbalance associated with machine learning classifiers, cautions are advised to ensure the reduction of false-positive rates [43]. Hence, predictions algorithms are recently being explored since it also supports real-time analysis applicable to preventing smart systems from cyberthreats.

Cyberthreats are capable of causing major breakdown to AMI security requirements [9] which could lead to complete system collapse by allowing illegal alterations through systems’ functions [3]. This has caused a major concern globally in SGs data security

Fig. 2 Modes by which electricity thefts occur in AMI

Fig. 3 Smart city energy management scheme

This is an open access article published by the IET under the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/)
which poses severe threats to power systems' operations. Man-in-the-middle (MiM) attacks, DoS attacks and other data injection/manipulations are capable of manipulating the state estimation by altering state variable and measurements [18]. For instance, this could cause false outage information increasing the period for fault location and operational costs [9].

AMI faces several cyberattacks necessitating increased research in this area. Some of which include a cyber-related study by [10] on how DoS and MiM are exploited in a given local area network to launch negative effects on SEMs. The author presented how caches of attackers corrupt SEMs entries via the address resolution protocol. This is a DoS attack, which cripple systems' functions thus interrupting its communication with other network hosts. In [2], an attack tree model for AMI was investigated based on security requirements and systems' model. In [3], a threat model for SG security was presented based on the technical and non-technical sources of threats with a proposed model for security implementation. In an improved model, a multi-layered threat model and analysis were given based on evaluation of cyber-physical systems (CPSs)' vulnerability metrics [50].

Some other reported techniques in literature include support vector machine, deep recurrent neural network (RNN), Lempel-Ziv algorithms, regression models, feasible generalised least squares models, integrated embedded system designed and developed for automation of the substation as a measure for clearing power theft, application of wireless data transmission and reception techniques employed for power monitoring and theft detection, a quantum key distribution model for a cloud-based security of the AMI, GSM-based prepaid energy meter presented to curb meter bypass, temperature-dependent predictive model which uses smart meter data and data from distribution transformer to detect electricity theft in an area, reconstructed user load profile using compressed distributed sensing based on random walk to demonstrate monitoring of customer's consumption for possible electricity theft, advanced wireless technology for monitoring of power theft, predictive models for TLs in electrical distribution networks [4, 19, 38, 41, 49, 51–57] etc.

Whatever the mode of attacks, there is need for proactive monitoring to enable timely intrusion detection. In [41], a monitoring framework based on GSM technology for the real-time energy theft detection was presented. The author, however, suggested a system of monitoring capable of reporting unexpected events using prepaid energy meter data. Manual inspections are also being carried out to address this unfortunate menace as reported by [58] where many illegal connections through walls and undergrounds were reported. In an effort aimed at reducing human efforts in energy management scheme, cloud-based monitoring of smart meters by both customers and utilities was presented in [59]. When cloud-based data automated with the application of IoTs have also been reported and are thought of as a means of enhancing the security [60–64] but are still subject to cyberattacks.

Other managerial approaches such as monitoring of customer meters and its data, restructuring of power systems ownership, policy formulations, regulations and implementations etc. have been suggested and practised. Moreover, tamper-evident seals are easily outdated while most adopted techniques only signify theft activity without localising the consumer [39]. Also mitigating against the deployment are the high cost of SEMs, unnecessary bureaucracies with lots of bottlenecks in the mass roll-out and installations etc. [65].

The highlight of available work shows that more efforts are concentrated at analysing consumption data to detect electricity theft. Although few works have attempted to proffer solutions based on intrusion detection techniques, no consideration has been given based on the sources causing electricity thefts. Therefore, further research works based on real-time identification of the source of threats is needed for efficient monitoring and control. This will ensure timely detection of threats for necessary actions long before the major setback is inflicted on the system. To provide for electricity theft detection by sources of threats, it is exigent to study AMI security requirement and its sources of threats.

5 AMI security requirements and sources of threats

Attacks on SEMs are basically aimed at the manipulation of its data and are a major concern as it is exposed not only to the revenue to jeopardy but also to the customers' privacy. It is also capable of inflict negative effects on the overall power grid operations [10]. Luckily, these attacks and other fraudulent related activities such as illegal procurements, sale and compromised installations by utility staff, connivance with customers usually by third parties to commit electricity thefts, illegal buying and selling of prepaid voucher etc. manifest by the presence of corrupt data in the AMI, hence, can be analysed and inferred with the aid of machine-learning techniques.

As depicted in Fig. 4, the security requirements for managing AMI data just as similar to data in general, are viewed in terms of [16, 29, 66, 67]:

(i) Access control: This determines the measure guaranteeing that only set access keys and controls are recognised and must be flexible for alteration at any time.

(ii) Analysis and feedback: This is an all-important function of the AMI and a measure of the systems' ability to evaluate itself and attempt self-healing. AMI systems must be able to achieve automated control based on any internal or external disturbance and communicate these records for further possible analysis and inferences.

(iii) Authentication: This is the evaluation of the requirement that data can be confirmed by all authorised entities to be as specified and ensure normal operations.

(iv) Authorisation: This demonstrates that only certified entities are empowered to access or operate control the system and breach whatsoever is allowed.

(v) Availability: This is a measure of the requirements showing the fact that authenticated data are available to authorised personnel whenever they are needed. When needed, any failure of the system's inability to make the required data available is not entertained. Moreover, the system must always operate correctly and should minimise downtimes as much as possible even in the event of attacks.

(vi) Confidentiality: This is a measure of a key requirement ensuring that protected data is only accessible to authorised persons, operators, organisation or any specified entity in general. To achieve this requirement, the AMI must ensure that intentional or unintentional breach or disclosure of any aspect of the data does not occur. The AMI must ensure customer data are well preserved such that unauthorised entities do not have access to it. In other words, its privacy must be well protected and confidential.

(vii) Integrity: This is AMI's requirement of authenticity, correctness and a true reflection of a system that does not allow unauthorised modifications to any aspect of the data by any means. It is an evaluation of the fact that the system can be trusted without doubts and must detect every illegal activity. The information flow between any members of the AMI architecture must be authentic and trusted.

(viii) Non-repudiation: This is a requirement indicating that only authorised entities receive data and do not deny receiving it where they did just as there won't be a claim of such receipt if there was none. In summary, no false alarm of information interchange is entertained, i.e. any action by the AMI cannot be denied by any party.

(ix) Privacy: The security of the systems' data must be guaranteed from every unauthorised entity. In addition, customers must be certain of the safety of their profile from hackers or any unauthorised entity. Where confidentiality is a measure of trust on the security of the data, the privacy is more of the measure of this trust by the customers.

(x) Accountability: This is AMI's requirement that all actions taken by the system are verified and undeniable. It is also termed to be the same as non-repudiation.
Generally, AMI basic requirements are confidentiality, integrity, availability and non-repudiation (CIAN). However, maintaining CIAN is threatened due to activities of cyberattackers, who in this case, mostly aim to undermine the AMI for electricity theft. These threats to AMI’s CIAN can be checked by two approaches, viz; ensuring the security requirements of the AMI is sustained and restored immediately after any successful attack or by proactive identification of the sources of threats and subsequent application of relevant models and algorithm for control of the requisite systems' parameters. Note that an indication of breach or threat means the loss of any of the CIAN’s requirements but analysis of the attacks and attackers give better insights [53] for proper monitoring and control of the system.

AMI threats can be viewed from three basic sources according to [9, 12], but this study has identified and categorised the threats into four groups: the primary source, the intermediate source, Nation (or State) threats and environmental (or natural hazards), as depicted in Fig. 4. As evident, depending on the observed source of threats, the AMI can be undermined by various activities, but this study focuses on those threats contributing to electricity thefts. Coincidentally, they form the major chunk of the threats to AMI.

The primary threats are traced to the customer end, utility or insider threats and community threats. Fig. 4 highlights some of the possible means by which these threats can malign the AMI. The main aim is to manipulate the recorded load or billing data to either reflect or capture a minimised cost compared to the actual value or even totally evade payments. While the customers may not be too sophisticated even though a larger percentage of theft activities come directly from them, the insider or utility threats can dent a huge blow. The insiders are technically inclined and have authorised access making them serious threats where they are compromised. The insiders could be AMI headend controllers, network administrators, managers of certain entities etc [67].

The intermediate threats are those traced to third parties who are majorly the network support providers. Compromised operators of this category are also sometimes classed as insiders since they have some authorised access to the system.

Nation or state to state threats are often not aimed at electricity theft, rather, to cause system breakdown or total collapse in an attempt to force those nation(s) to obey a certain decision. Terrorism is another major threat under this category but is often due to insurgency of sought. Environmental or natural hazards are also of major concerns but are not the focus of this work.

Whatever the source of threats linked to electricity thefts, the primary aim of the attackers is to achieve economic gains by falsification of metering information [67].

To clear these threats, this work proposes a framework based on the manifesting symptoms observed by either loss of any of the security requirements or identified symptoms based on the sources of threats.

6 Modelling the threat monitoring and clearing scheme

The security of the AMI just as any other CPS relies on the cyber security. Cyber security measures help to sustain the CIAN of AMI against all the vulnerabilities posed by malicious threats. SGs necessitate a broad acquisition and analysis of data for vigorous and efficient management and operations [31] of smart cities. AMI being the centre of the communication between all stakeholders and facilities faces more threats hence, in this framework, data from SGs sensors and AMI are relied upon since they provide adequate data for useful analytics and application of various algorithms to detect faults, thefts and for decision support for improved systems [53].

A breach to any of the identified security requirement or sources of threats to AMI aimed at committing electricity thefts and are manifested by some known indicative symptoms. Some of these symptoms are summed up in Fig. 5. Fortunately, the SEM is designed to give alarms at the sense of most of the symptoms such as erratic outage notification, de-energised or SEM outage etc.
must be taken. A typical proactive measure will offer a real-time monitoring, clearance and possibly, further analysis to offer desired defence action. These are mostly achieved by studying the attack behaviours and threats as well as implementing an interconnected protection scheme, some of which are presented in [2, 3, 36, 39, 68–70], just before major losses are incurred.

In SEMs data, false consumption pattern may be manifested by:

(i) Frozen consumption values for a set timesteps.

(ii) High prediction error of the consumption data based on anomaly detection technique.

Frozen consumption values are where observed consumption values remain unchanged for a set number of timesteps. Usually, SEMs recorded consumption data are usually in a minute step but to give an appropriate period of flagging any possible threat, recorded data at 30 min interval may be considered for each time step and errors are only flagged after a set number of timesteps, frozen consumption pattern is observed. Fig. 6 shows a typical trend of a frozen consumption pattern. The figure shows that from the 190th timestep, the consumption value did not only significantly reduce but remained at the same value for the next over 10 steps. This is enough to trigger suspicion for further analysis. There may be no cause for alarm if from the central observer meter for the neighbourhood to which the customer belongs, there is no sign of theft.

To determine the prediction errors, each customer consumption data is treated as a time series data with the data randomly recorded based on the set period for each timestep, say at 30 min interval. The first three weeks data amounting to 1008 datapoints is just enough to be split for training and testing to predict for the next, say, 5 days (using about 75:25 training to test ratio using any suitable machine-learning model such as neural networks (NNs) for time-series predictions, RNNs or even the higher versions such as long short-term memory (LSTMs) networks and its variants which have been proven to take care of vanishing gradients observed in NNs and RNNs. As applied to all the time series data, given a set of consumption data, say, \( e_1, e_2, e_3, \ldots, e_n \), the aim is to predict the next consumption value, \( e_{n+1} \), depending on the number of set timesteps \( j \). Fig. 7 shows a prediction model achieved using an LSTM network. The predicted timesteps data are compared with the true recorded data to determine anomaly using any suitable distance-based method. In the anomaly regions 1, 2 and 3 as indicated in Fig. 7, the prediction errors are high. If the timesteps to flag error is not allowed to go beyond, say 5, the customer would have been reported for further analysis long before any other anomaly. If the flagging timesteps is, say, 10, all the anomaly regions or even more may surface. This is, however, not enough to conclude that electricity theft has taken place, but it is enough as a cause for further analysis. So, the utility operators must decide a favourable value of timestep to flag further analysis. The value of the flagging timestep depends on the period of each timestep, the theft history of the neighbourhood the customer belongs and the revenue status.

6.2 False signature on energy consumption data

This is another result of cyberattack achieved either by false data injection attacks (data corruption), loss of data, stealing of data or even swapping of data. False data injection could lead to lower values of energy consumption or lower values of the billings. Attackers could also aim to swap customers' data just as the physical meters were reportedly stolen and swapped in the conventional metering. Although, that is not possible with the deployment of AMI, swapping of customers' identity is another worrying issue. This is a critical issue in smart metering as attackers aim to disrupt the true state parameters leading to unhealthy records of SEMs. Intrusion detections, phasor measurement units based protection and real-time state estimation...
techniques are employed to help prevent any form of meter data manipulations. Several inferential analyses are also carried out on a regular basis at the AMI's headend to monitor and prevent false signatures on the SEM data.

6.3 False billings

False billings are another strategy employed by attackers as a means of evading payment for energy consumed. This is achieved by manipulating the price regime to reduce by a set percentage or by a fixed low price which will never vary as opposed to the real-time pricing (RTP) scheme of the SGs. However, it is sometimes, difficult to determine when the price regime is tampered by using a single customers' data. This is because the RTP in some cases may remain unchanged for given hours of day over a considerable long period of time. To authenticate the true pricing, constant comparisons of the values as seen by each meter in each neighbourhood are compared and with the values from at the utility end. Let \( p_{1,j}, p_{1,2}, p_{1,3}, \ldots, p_{1,j} \), \( p_{2,j}, p_{2,2}, p_{2,3}, \ldots, p_{2,j} \), \( p_{3,j}, p_{3,2}, p_{3,3}, \ldots, p_{3,j} \) be the instantaneous price regime as applied to the neighbourhood at timesteps 1, 2, 3 to \( i \), respectively. Then, at any given timestep, (1) is formulated for ensuring constant monitoring among customers while (2) is used to compare any given customers' billing data with those as given from the utility

\[
\sum_j p_{1,j} = \sum_j p_{2,j} = \sum_j p_{3,j} = \ldots, \sum_j p_{i,j} 
\] (1)

\[
\sum_j p_{u,j} = \sum_j p_{u,j} 
\] (2)

where \( p_{u,j} \) denotes the billing as set by the utility at timestep \( j \).

Fig. 8 shows a sample false billing by a potentially fraudulent customer. The figure shows the energy consumption profile and its corresponding RTP. From the 314th timestamp, the RTP becomes frozen and never changes again for a considerable long time of timesteps. However, (1) and (2) are needed to make the final decision of the level of threats.

6.4 Framework for clearing the threats

To clear any identified threats, the AMI systems' backend analyses are relied upon using authenticated system data for verification. Fig. 9 gives the detailed framework for monitoring and control based on identified maturing symptoms manifested in the obtained data from sensors and meters using relevant techniques. Suitable machine learning algorithms are applied on the obtained data for easy inferences and the source of threat to energy efficiency through energy theft is then traced for clearance, identification and report of possibly threatened SEMs.
leading to electricity theft can be addressed. Future works may explore extensively, each of the identified sources of threats and application of suitable intelligent algorithm on a test data for implementation of the framework for a real-time decision support.

8 Acknowledgments

The authors are grateful to PROUDLY ANEBIRA for their financial support.

9 References

[1] Ejaz, W., Naeem, M., Shahid, S., et al.: ‘Efficient energy management for the internet of things in smart cities’, IEEE Commun. Mag., 2017, 55, (1), pp. 84–91
[2] Jang, R., Lu, R., Wang, Y., et al.: ‘Energy-theft detection issues for advanced metering infrastructure in smart grid’, Tsinghua Sci. Technol., 2014, 19, (2), pp. 105–120
[3] Otoze, A.O., Mustafa, M.W., Larik, R.M.: ‘Smart grids security challenges: classification by sources of threats’, J. Electr. Syst. Inf. Technol., 2018, 5, (3), pp. 468–483
[4] Delgado-Gomes, V., Martins, J.F., Lima, C., et al.: ‘Smart grid security issues’. 2015 9th Int. Conf. Compatibility and Power Electronics (CPE), 2015
[5] Amin, S.M.: ‘Smart grid security, privacy, and resilient architectures: opportunities and challenges’. Power and Energy Society General Meeting, 2012 IEEE, Manchester Grand Hyatt, San Diego, California, USA, 2012
[6] Abdurrahman, T.A., Isiwekpeni, O.H., Surajudeen-Bakinde, N.T., et al.: ‘Design, specification and implementation of a distributed home automation system’, Proc. Comput. Sci., 2016, 94, pp. 473–478
[7] Kramers, A., Höjera, M., Lövehagen, N., et al.: ‘Smart sustainable cities–exploring ICT solutions for reduced energy use in cities’, Environ. Model. Softw., 2014, 56, pp. 52–62
[8] Jin, J., Grabi, J., Marusic, S., et al.: ‘An information framework for creating a smart city through internet of things’, IEEE Internet Things J., 2014, 1, (2), pp. 112–121
[9] Jokar, P.: ‘Detection of malicious activities against advanced metering infrastructure in smart grid’ (University of British Columbia, Canada, 2015)
[10] Shuaib, K., Trabelsi, Z., Abed-Hafez, M., et al.: ‘Resiliency of smart power meters to common security attacks’, Proc. Comput. Sci., 2015, 52, pp. 145–152
[11] Fatemieh, O., Chandra, R., Günter, C.A.: ‘Low cost and secure smart meter communications using the TV white spaces’. 2010 3rd Int. Symp. on Resilient Control Systems (ISRCS), Idaho Falls, Idaho, USA, 2010
[12] Jokar, P.: ‘Detection of malicious activities against advanced metering infrastructure in smart grid’ (University of British Columbia, Canada, 2015)
[13] Siano, P.: ‘Demand response and smart grids – A survey’, Renew. Sust. Energy Rev., 2014, 30, pp. 461–478
[14] Geelen, D., Reinders, A., Keyson, D.: ‘Empowering the end-user in smart grids: recommendations for the design of products and services’, Energy Policy, 2013, 61, pp. 151–161
[15] Khattak, A.M., Khanji, S.I., Khan, W.A.: ‘Smart meter security: vulnerabilities, threat impacts, and countermeasures’. Int. Conf. on Ubiquitous Information Management and Communication, Phuket, Thailand, 2010, Springer
[16] Cleveland, F.M.: ‘Cyber security issues for advanced metering infrastructure (AMI)’. 2008 IEEE Power and Energy Society General Meeting-Conversion
