VOL. 14, NO. 19, OCTOBER 2019 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

ENERGY THEFT DETECTION IN MULTI TENANT DATA CENTERS AND DISTRIBUTION LINE USING SMART GRIDS

M. Sivarathinabala[1] and T. Niruban Projoth[2]
[1]Department of Electronics and Communication, Velammal Institute of Technology, Chennai, India
[2]Department of Mechanical and Construction, Veltech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Chennai, India
E-Mail: sivarathinabala@gmail.com

ABSTRACT

In recent years, High performance data centers are one of the challenging research areas in Cloud Computing. Multi Tenant Data centers are the infra structures that runs in large-scale Internet-based services. Energy consumption models are pivotal and efficient in designing and optimizing energy-efficient operations to curb excessive energy consumption in the data centers. Multi-tenant data centers (MTDCs) are the data centers which are popular with different operational structure. Despite the offered benefits, MTDCs are vulnerable to various cyber attacks. An important cyber attack is energy theft which can be launched by malicious tenants to reduce cost of the electricity consumption by attacking their own smart meters or neighboring meters to undercount its energy usage. Billions of money has been lost due to energy theft in data centers each year. Localization of energy theft detection is an effective way to limit the labor cost in detecting energy theft in data centers. It can be facilitated through deploying Digital Protective Relays (DPR) in the Power Distribution Unit of the data center. DPR is a microprocessor based device for fault detection. Along with DPR, an anamoly identification algorithm has been implemented called as Minimum Covariance Determinant .The smart meters along with Advance Metering Infrastructure is employed to measure the energy consumption of the tenants in data center, which is implemented in Smart grid environment. Such that data from both smart meter and Digital Protective Relay is send to the utility center to determine the Energy Theft in Multi Tenant Data Centers.

Keywords: anamoly detection, cloud computing, multi tenant data center.

1. INTRODUCTION

In this paper, energy theft occurs in Multi Tenant Data Centers and energy theft [1-3] occurs in the distribution line from the smart grid such that various methods have been employed to detect the energy theft. Cloud computing vendors and multi-tenant collocation facilities are used to maximize the scalability, efficiency and performance of their data centers. The power configurations are closely supervised by their customers who are comparing to them with the other service options in a very competitive environment. Theft of electricity is the crime and it is meant by stealing of electrical power. It is a crime and is punishable by fines and/or incarceration. It belongs to the non-technical losses in data centers. India loses billions of rupees because of unbilled consumption and unlawful usage of electricity such that data center also loses billions of money per year. A Multi-Tenant Data Center (MTDC) is a type of data center which rents physical space to customers in a shared building while providing logistical services, such as physical security, power management and cooling, a multi tenant data center (MTDC) has become popular for various internet service providers and cloud computing platforms, Multi-Tenant Data Center (MTDC) is a type of data center where physical space, power supply and maintenance services are available for rental to customers. The architecture for Multi Tenant Data Center is given below: it makes use of smart meters, Advanced Metering Infrastructure with intrusion detection system ,Digital Protective Relay, MCD Anamoly detection Algorithm, RFID, Microcontroller, GSM , sensors, smart grid environment. Malicious tenants may attack their own smart meters to reduce the electricity usage. As the result the smart meter reports an erroneous energy usage reading lower than the actual one to the Utility Company. Advanced Metering Infrastructure (AMI) is one of the essential components in the smart grid which replaces the analog meters with computerized systems that report usage over digital communication interfaces.

2. ENERGY THEFT AND SMART GRID

Generation, transmission and distribution of electrical energy may involve many operational losses. Whereas, losses implicated in generation can be technically defined, transmission and distribution losses cannot be precisely quantified with the sending end information. .Energy theft [8] can be difficult to identify and pinpoint the theft in data centers.Like any Criminal activity ,methods shift constantly as utilities develop counter measures. Electric utilities lose large amounts of money each year due to power theft by electricity consumers. Electricity power theft is the use of electricity equipment or service in illegal manner in order to avoid billing charge. It is difficult to distinguish between original and fake customers.

Smart grids [12] are an integrated communication and power system infrastructure used in distribution lines which allows for robust to a communication, and distributed computers to improve the efficiency, reliability and safety of power delivery and use. Smart grid technology helps for developing countries in the growth of their power sector. Smart grid in energy transmission means use of feedback from the consumption end. Electricity stealing is a long term problem in our country.

However, in power supply department huge investments of manpower and material, as stealing of electricity has been increased the phenomenon of defending stealing electricity has increased.

3. EXISTING SYSTEM

A Multi-Tenant Data Center (MTDC) [4-6] is a type of data center which rents physical space to customers in a shared building while providing logistical services. Compared with traditional owner-operated data centers, both the deployment complexity and the maintenance cost are minimized in the data centers. The high availability of MTDCs is made possible by both the external sources and internal power sources. It relies on the internal power source, including uninterrupted power supplies (UPS), and power distribution units (PDU). UPS is responsible for delivering power to the PDUs .At the low level of the distribution network, each PDU has the capacity in the range of 200kW to 300 kW while supplying power to the minimum of around 50 racks .The power demand of an individual tenant varies from a few kW to several hundred kW, depending on the number of machines owns. To improve the availability, in certain architectures, each PDU might be equipped with its dedicated UPS. The target is to insert the minimum number of DPRs into the network for monitoring the energy usage of the tenants in data centers. Each Power Distribution Unit (PDU) delivers electricity to a set of tenants and each tenant is equipped with a smart meter, which reports the energy usage to the utility company periodically for billing purposes. Data centers provide strong incentives for malicious tenants to attack their own smart meters in order to reduce the monetary cost on electricity usage. Each tenant is assigned an overall anomaly rate, which is compared with a random number generated at each time slot to determine whether it commits energy theft at that time slot. In a Multi Tenant Data Center each and every tenant is provided with smart meter and Digital protective relay with MCD anamoly detection algorithm.

The purpose of the smart meter is to record the energy consumption of each and every tenant and sends the data to the utility center. In the Power energy transmitted and energy consumption of every tenant and sends the data to the utility center. The Utility center compares the data from both DPR and smart meter and determines whether the energy theft is occurred or not in the data center. If an energy theft is occurred in a data center, utility center will take necessary actions to eliminate the energy theft.

Distribution Unit, the purpose of DPR is to determine the the various types of electrical power theft in distribution line from smart grid include: Direct hooking from line, Bypassing the energy meter - involves hooking directly into power line ahead of the meter, or short circuiting the input/output terminal to prevent energy from registry. Slowing down other meter - Physical objects or magnets are sometimes used to slow down a meter, while more advanced methods involve installing a foreign circuit that can be controlled remotely to avoid easy detection and injecting foreign element into the energy meter.

4. PROPOSED SYSTEM

A smart meter is proposed that sends the meter readings digitally to individual supplier for generating the accurate bills. Smart meters come within home displays, so you can better understand energy usage. Smart meters are widely employed in smart grid in order to determine the electricity theft. Smart meters records how much energy is consumed by the consumer for every thirty minutes and sends the data to utility center. Digital Protective Relays (DPR) in the data center where a DPR is a microprocessor based device for fault detection and event logging in the power system. Due to the large scale of the power distribution network of the data center, it is a non-trivial task to optimize the physical locations for DPR insertions. The anomaly rate of a smart meter is defined as the percentage of time slots associated with energy theft in all time slots. As the number fluctuates over time, it is difficult to generate a DPR insertion solution that remains of high quality in the long term. Inserting a DPR to monitor them might not be ideal if their anomaly rates drop in the future. For this purpose DPR is inserted into group of Power Distribution Unit. With the server management services deployed by the tenants, the number of active servers fluctuates with the amount of workloads. This causes the difficulty in identifying energy theft given the historical record of energy usage of each tenant. An intelligent Minimum Covariance Determinant (MCD)-based anomaly identification algorithm has been proposed to detect anamoly.

Our algorithm inserts the minimum number of DPRs into the power distribution network of the data center. In addition, our DPR insertion solution explores an innovative aggregated anomaly rate range which accounts for the long term effect of energy theft in an MTDC. The advanced metering infrastructure (AMI) is the sensor network in the smart grid. It provides the information about energy usage (demand) to utilities, consumers and the grid itself. It is a two way communication. This makes all parties to conclude better decisions about costs and strain on the grid during times of peak demand. Smart meters perform four basic functions with respect to power management; a) the monitoring and recording of demand, b) the logging of power relevant events, e.g., outages, c) the delivery of usage and logging information to the upstream utilities, and d) delivering and receiving of control messages, e.g., controlling smart appliances, remote disconnect, etc. AMI enables a number of services related to demand measurement. Meters supporting automatic meter reading (AMR) can report demand to utilities automatically via communication networks. Time-of-use (TOU) pricing refers to a pricing scheme in which power costs more during hours of peak demand. TOU schemes divide a day into several partitions called tariffs, typically peak and off-peak. Finally, customers are motivated to reduce costs by moving some energy-intensive tasks to off-peak hours, reducing the peak strain on the grid.

The smart grid refers to the modernization of power grid infrastructure with new technologies, enabling more intelligently networked automated system with the goal of improving efficiency, reliability, and security, providing transparency and choices to electricity consumers. AMI refers to the modernization of the electricity metering system by replacing old mechanical meters by smart meters. Smart meters are new embedded devices that provide two-way communications between utilities and consumers. An Advanced Metering Infrastructure (AMI), proposed an architecture that communicates from smart meter to grid using meter to meter communication. The utility companies can also provide faster diagnosis of outage and dynamical electricity price thanks to the AMI. Hence, AMI has attracted great attention from many stakeholders, including utility companies, energy markets, regulators, etc. RFID technology can be used to detect energy theft; the utility companies have to pay extra cost to install the system. In order to find out whether implementing RFID technology is beneficial for the utility company, cost-benefit theory is used to analyse different value changes caused by the proposed system. Radio Frequency IDentification (RFID) technology to help the electricity supply company deal with its ammeter inventory management and prevent energy theft. There are two parts in the proposed system: ammeter inventory management and ammeter verification control. The ammeter inventory management includes an RFID tag on each ammeter, RFID readers, the middleware, and the network with the Enterprise Resource Planning (ERP) system of the electricity supply company. The integrity of the RFID tag can be used to detect energy theft. With the development of advanced metering infrastructure in smart grid, more complicated situation in energy theft has emerged and many new technologies are adopted to solve this problem.

5. ENERGY THEFT DETECTION IN DISTRIBUTION LINE FROM THE SMART GRID

Smart grid [7] is a new generation of electrical grid communication with high management of power flow control, self-healing, energy efficiency, security through digital communication networks and technologies .It is the integration of electrical power grid and ICT which is developing all over the world, it is a fully sustainable form of reliable and electrical energy in existing network with advanced technologies. The power supply from the smart grid, Generator, UPS is fed into the Multi tenant data center.Such that energy theft may occur in the transmission line. The power supply from the source (smart grid) is passed to the Current Transformer at the load side because high current cannot be handled by a meter. A Current transformer is placed at the Transmission side. And the Arduino based microcontroller is placed such that it handles both the current transformer at the load side and current transformer at the transmission side.

When the total amount of energy transmitted by the power supply is not equal to the energy consumed then the energy theft is occurred in the distribution line. The information is sent to the Arduino (microcontroller) such it determines the energy theft has been occurred in the distribution line.GSM has been highly employed [9,10,11] and it is integrated with the microcontroller, such that the message is sent to the mobile number in the utility center which is stored in GSM when the energy theft is occurred in the distribution line.

5.1 Energy theft detection within MTDC

Smart meters along with Advanced metering Infrastructure are widely used to monitor the electricity consumed by the consumers and the data is sent to the utility center for every thirty minutes. It provides the two way communication between the consumers and the utility center.The Digital Protective Relay in Power Distribution Unit is used to monitor how much energy is transmitted into the system and how much energy is used by the tenants.

Both DPR and smart meter sends the data about the energy usage of the tenants to the utility company. When the energy transmitted in MTDC is not equal to the energy consumed then the energy theft is occurred in MTDC. The malicious tenants may attack their smart meter in order to reduce the consumption rate.

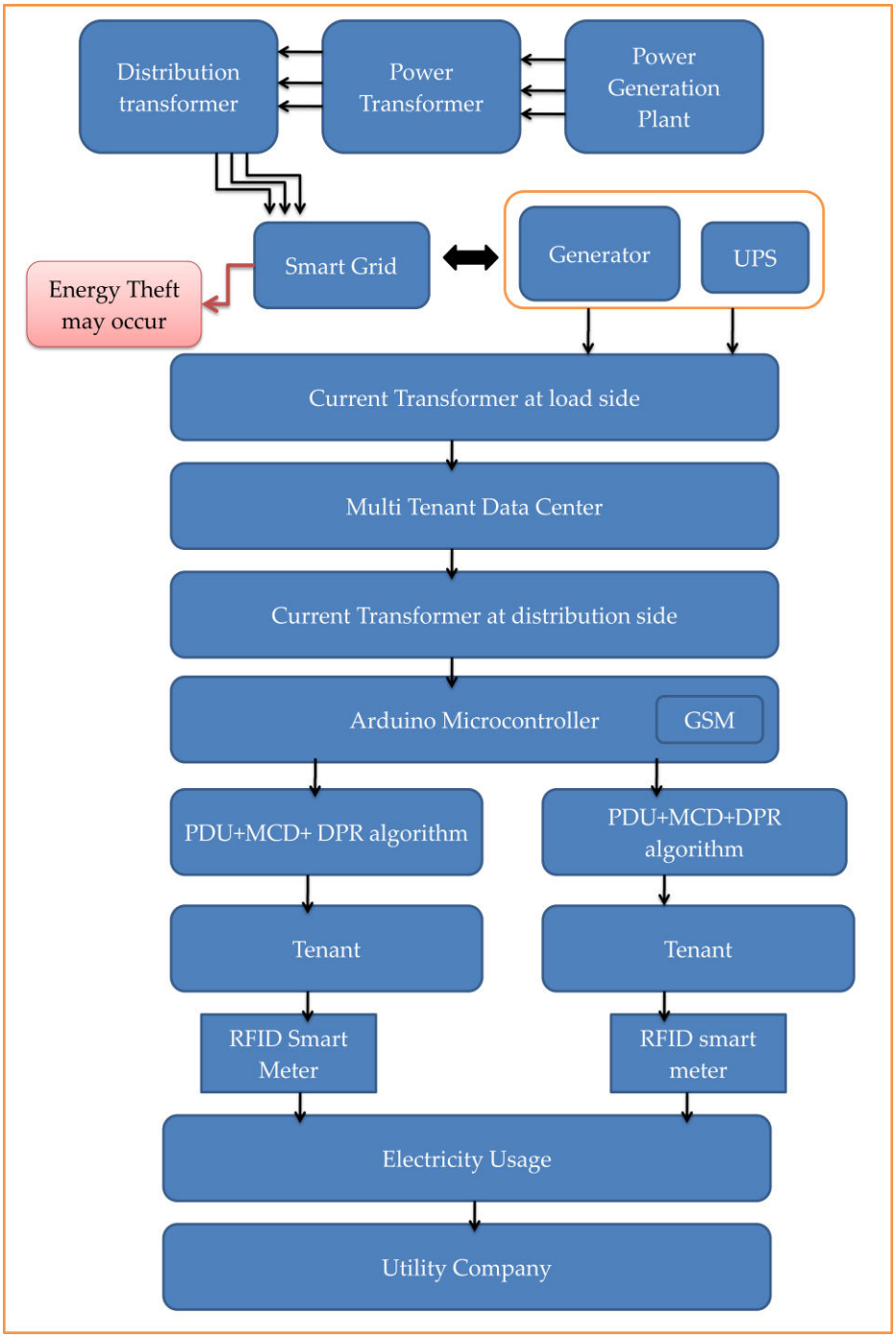

Figure-1. Architecture of MTDC.

5.2 Architecture of MTDC

The Figure-1 shows the architecture of multi tenant data center. Each smart meter is provided with an RFID tag to help the electricity supply deal with its ammeter to prevent energy theft. AMI is provided with Intrusion Detection system that uses the information fusion to combine the sensor and data from smart meter to more accurately detect energy theft.

When the smart meter sends the electricity usage to the utility company it determines whether the data is sent by original RFID or not. Zigbee is the high speed wireless communication network. It has the transceiver module which will receives each consumer load transmitted from consumer unit. It provides the communication between the smart meter and the utility company. Thus whenever energy theft happens in the transmission line from Smart grid, the data is send to the utility company informing that the energy theft has been happened in the transmission line by sending the message through GSM.Whenever energy theft occurs within the Multi Tenant Data Center, Smart meter along with AMI sends the data to utility center for every thirty minutes. The DPR in the power distribution unit records the energy transmitted and consumed if the data sent by both DPR

and Smart meter are not equal to each other, and then the energy theft is occurred in multi tenant data center. Then the Utility center takes necessary actions to overcome such thefts. Figure-2 shows the working of smart meter.

6. PROPOSED MCD ANAMOLY IDENTIFICATION ALGORITHM

MCD [13,14] is a robust estimator of the location and covariance of a given data set and is widely used as an anomaly detection algorithm. It is achieved by selecting a subset of h data points from the original data set such that the covariance matrix of the subset has the minimum determinant. Subsequently, the Mahalanobis distance is calculated for each data point to determine its distance to the distribution. It is clear that the data points with significant distance from the distribution can be identified as anomalies. Mathematically, the Mahalanobis distance is defined as

$$M|D(x_i) = \sqrt{(X_i - T_0)}' S_0^{-1} (X_i - T_0) \qquad (1)$$

in which x_i is one data point. T_0 and S_0 are the arithmetic mean and the covariance matrix of the data set. It measures the number of standard deviations that the data point x_i is away from the mean of the distribution characterized by T_0 and S_0. Since the original data set contains anomalies, T_0 and S_0 calculated from the original data set is not accurate. MCD algorithm maintains and optimizes a subset of h data points iteratively such that T0 and S0 can be accurately estimated.

The key operation of the MCD algorithm is C-Step. It starts from a given subset $H_{old} \subset X_n$, with h elements selected from the original data set $X_n = \{X_1, X_2, \ldots\ldots, X_n\}$. The arithmetic mean of the H_{old} is calculated as,

$$T_{old} = \frac{1}{h} \sum_{i \in H_{old}} X_i \qquad (2)$$

The covariance matrix is defined as

$$S_{old} = \frac{1}{h} \sum_{i \in H_{old}} (X_i - T_{old})(X_i - T_{old})' \qquad (3)$$

Given T_{old} and S_{old}, the mahalanobis distance of each data point in X_n can be calculated in similar fashion as in equation 1. They are subsequently sorted such that the permutation π of the data points can be obtained as

$$d_{old}(\pi(1)) \leq d_{old}(\pi(2)) \leq \cdots \leq d_{old}(\pi(n)) \qquad (4)$$

in which $d_{old}(\_)$ denotes the distance of each data point to the distribution characterized as T_{old} and S_{old}. The new subset H_{new} can be obtained by selecting the top h data points with the minimum distance from the permutation,

$$H_{new} = \pi(1), \pi(2), \ldots\ldots, \pi(h) \qquad (5)$$

Subsequently, the arithmetic mean and covariance matrix of H_{new} is calculated in the same fashion as in Eqn.5, respectively. It is guaranteed that $\det(S_{new}) < \det(S_{old})$, in which $\det(\_)$ is the determinant of the covariance matrix. It indicates that the data points in H_{new} are less sparsely.

7. CONCLUSIONS

Energy theft in MTDCs is highly undesirable in the era of sustainable computing as it encourages overuse of energy for the cloud service providers. When energy theft occurs in an MTDC, the data center operator could have to examine each smart meter in order to find the compromised ones. We have proposed an anomaly range based dynamic programming algorithm for inserting the minimum number of DPRs into the data center while still limiting the average number of tenants to be checked when energy theft occurs. Smart meter in smart grid along with Advanced Metering Infrastructure has been highly employed to measure the energy consumed by the tenants and the data is send to the utility company. Arduino is a Microcontroller it can control the smart devices connected to it such sensors and GSM. Both the current transformers at the load side and transmission side is managed and controlled by the Microcontroller. Thus the proposed network design identifies the energy theft in distribution line from Smart grid and data centers in more efficient manner. As the future work, the impact of different energy theft patterns on DPR insertion algorithm will be further studied. Anomaly detection algorithms will be proposed to handle various specific energy theft patterns, in which the malicious tenant attacks in both own smart meter and the neighboring ones.

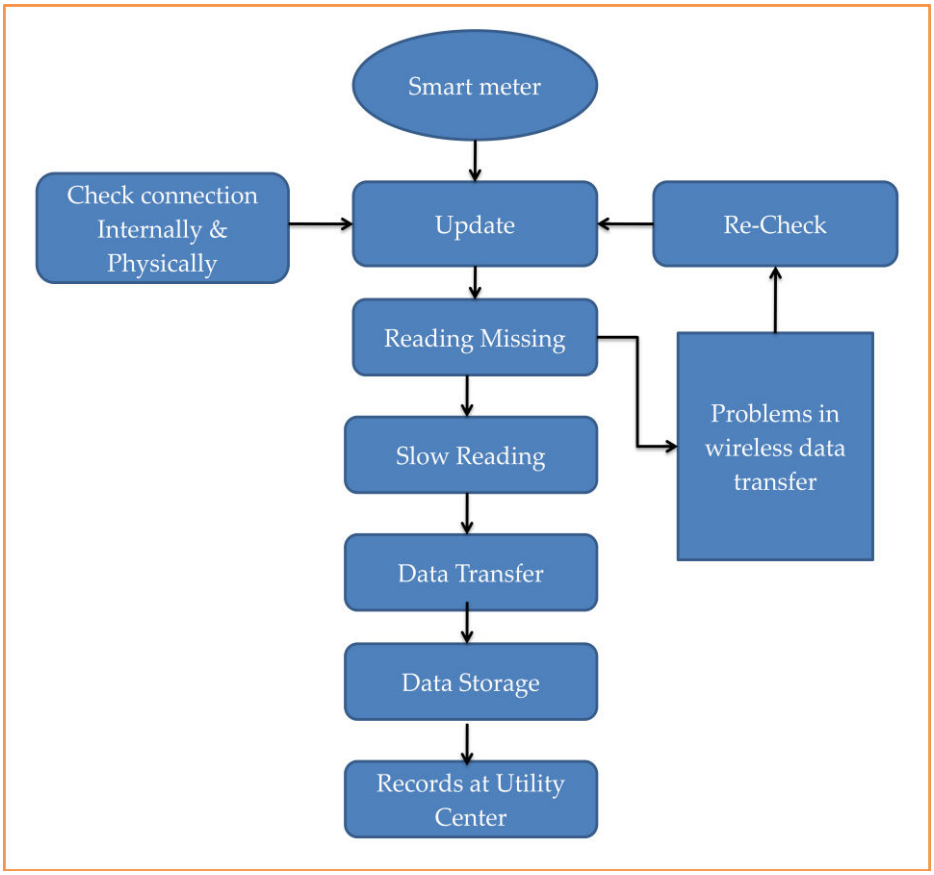

Figure-2. Working of Smart Meter.

REFERENCES

[1] M. A. Islam, X. Ren, S. Ren, A. Wierman and X. Wang. 2016. A market approach for handling power emergencies in multi-tenant data center. in Proceedings of IEEE International Symposium on High Performance Computer Architecture (HPCA).

[2] Natural Resources Defense Council. 2016. America's data centers consuming and wasting growing amounts of energy. [Online]. Available: http://www.nrdc.org/energy/ data-center-efficiency-assessment.asp

[3] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni. 2011. Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft. Energy Policy. 39: 1007-1015.

[4] S. McLaughlin, D. Podkuiko and P.McDaniel.Energy theft in Advanced Metering Infrastructure. Pennsylvania State University, University Park.

[5] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni. 2011. Smart meters for power grid: Challenges, issues, advantages and status. Renewable and sustainable energy reviews. 15, pp. 2736-2742.

[6] S. F. Bush. 2014. Smart Grid: Communication-Enabled Intelligence for the Electric Power Grid. IEEE Press, Wiley.

[7] K. Billewicz. 2012. Smart Metering: Intelligent measuring system. Original title: Smart Metering: Inteligentny system pomiarowy, PWN.

[8] Energa Operator, Theft of energy, illegal consumption. Original title: Kradziez energii, nielegalny pobor. Energa Operator Systemu Dystrybucyjnego, Online: http://www.energaoperator.pl/uslugi/kradziezenergii:xml; 2016

[9] R. Jiang, R. Lu, C. Lai, J. Luo and X. Shen, Robust group key management with revocation and collusion resistance for scada in smart grid, in Proc. IEEE Globe Communication Conference (Globecom), 2013, pp. 824-829.

[10] R. Lu, X. Liang, X. Li, X. Lin and X. Shen. 2012. EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid

communications, IEEE Transactions on Parallel and Distributed Systems. 23(9): 1621-1631.

[11] M. Wen, R. Lu, J. Lei, H. Li, X. Liang and X. Shen. 2014. SESA: An efficient searchable encryption scheme for auction in emerging smart grid marketing. Security and Communication Networks. 7(1): 234-244.

[12] Data Center Map. 2016. Colocation usa. [Online]. Available: http://www.datacentermap.com/usa/.

[13] P. J. Rousseeuw and K. V. Driessen. 1999. A fast algorithm for the minimum covariance determinant estimator. Technometrics. 41(3): 212-223.

[14] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed and M. Mohamad. Nontechnical loss detection for metered customers in power utility using support vector.

[15] Yip S.-C., Tan W.-N., Tan C., Gan M.-T., Wong K. 2018. An anomaly detection framework for identifying energy theft and defective meters in smart grids International Journal of Electrical Power and Energy Systems. Vol. 101.

[16] Viegas J. L., Esteves P. R., Vieira S. M. 2018.Clustering-based novelty detection for identification of non-technical losses International Journal of Electrical Power and Energy Systems. Vol. 101.

[17] Huang Y. C., Lin H. C., Huang Y. W. 2018.Application of the autocorrelation function to working-day calculation in power management Applied Soft Computing Journal. Vol. 68.

[18] Amr A. Munshi, Yasser A.-R. I. 2017. Mohamed Big data framework for analytics in smart grids Electric Power Systems Research. 151: 369-380.

[19] Yasin Kabalci. 2016.A survey on smart metering and smart grid communication Renewable and Sustainable Energy Reviews. 57: 302-318

[20] Yao Zhang, Wei Chen, Weijun Gao. 2017. A survey on the development status and challenges of smart grids in main driver countries Renewable and Sustainable Energy Reviews. 79: 137-147.

[21] Tanveer Ahmad, Huanxin Chen, Jiangyu Wang, Yabi n Guo. 2018.Review of various modeling techniques for the detection of electricity theft in smart grid environment Renewable and Sustainable Energy Reviews. 82(Part 3): 2916-2933.

[22] Soma Shekara Sreenadh Reddy Depuru, LingfengWang, Vijay Devabhaktuni. 2011.Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft Energy Policy. 39(2): 1007-1015.

[23] Sook-Chin Yip, Wooi-Nee Tan, Chia Kwang Tan, Ming-Tao Gan, Kok Sheik Wong. 2018. An anomaly detection framework for identifying energy theft and defective meters in smart grids International Journal of Electrical Power & Energy Systems. 101: 189-203.