A Security Study for Smart Metering Systems

Musaab Hasan, Farkhund Iqbal, Patrick C. K. Hung, Benjamin C. M. Fung, Laura Rafferty

***Abstract*—** In conjunction with the rapid growth in adopting smart devices, the smart cities concept has been raised simultaneously in many modern societies. A smart grid is an essential part of any smart city as both consumers and power utility companies benefit from the features provided by the power grid. In addition to advanced features presented by smart grids, there may also be a risk when the grids are exposed to malicious acts such as security attacks performed by terrorists. Many vendors develop smart meters and at the same time, many researchers have proposed various supported security systems, however, no security measures were considered in most of those designs. This paper presents a security study for smart metering systems with a prototype implementation for future works.

***Keywords*—** Security Design, Smart City, Smart Meter, Smart Grid, Smart Metering System.

I. Introduction

THE smart device concept provides an effective and efficient environment for our living; however, it also causes security concerns. For example, the Ukraine power grid system was attacked by hackers resulting in a disconnection of electricity of around 230 thousand people for a period reaching six hours in December 2015 [32]. In conjunction with the rapid growth in adopting smart devices, the smart cities concept has been raised simultaneously in many modern societies. Nowadays smart grids are an essential part of the smart city as they provide enormous features that enhance the consumer as well as power utility companies experience. In addition to the great features presented by smart grids, there may also be a risk when the grids are exposed to malicious behaviors such as security attacks performed by terrorists [1]. On the consumer side, multiple vendors were found to be developing and manufacturing advanced smart metering systems that play an essential role in smart grids. The simplest smart meters that can be found on the market include the functionalities of monitoring, recording the energy consumption and presenting the readings to the consumers in a user-friendly way to allow them to manage their consumption by reducing the usage of the appliances that consume high energy [2]. Generally, this type of meter is installed on the consumer side and the power company may have no control over it[3]. More advanced smart meters that are installed and maintained by the power companies involve having a two-way communication between the consumer meter and the power company [4]. This includes transferring data and usage information back and forth eliminating many tasks that are performed manually.

Smart meters are exposed to various types of attacks that could be launched from different parties even from the consumer side as most of the industrial meters are lacking advanced security measures [3][4]. Having a device that is connected to the power grids and located on the consumer side may encourage some of the attackers to perform illegal acts by either stealing energy or even hacking the main grid systems through their home smart meter [10]. Up to our best knowledge, there is not much research work in security measures on smart metering system designs [58].

The purpose of this research is to propose a security design for smart metering systems. This paper presents a study for a three-phase smart metering system design based on the consideration of common vulnerabilities from related research works. One of the major objectives is to ensure that the consumption data is delivered to the consumer and the power utility company securely without getting it sniffed or altered. The proposed design of the smart meter discussed in this paper is estimated to be consuming 1.5KW per month running for 24 hours. This amount of power was maintained by the careful selection of the electronic components and communication mediums used by the system. Referring to Figure 1, the limitations and features of the industrial products that are available in the market as well as the related work presented by other researchers were identified and combined to act as a baseline for our design. Maintaining the security of the system is essential to our design where common threats and attacks occurred to actual systems as well as those that have been experimented by researchers in a lab environment where identified and combined to list the possible threats and attacks to our system. The current system features and the possible threats and attacks were also considered in all the stages of the design and implementation to ensure the system has advanced features with ensured system compatibility and security.

M. H. is Pursuing M.S in Cyber Security at Zayed University, Abu Dhabi, UAE, and he is with the Electrical Engineering Department, Ajman University, Fujairah, UAE, (e-mail: m80006988@zu.ac.ae).

Farkhund Iqbal is with the College of Technological Innovation, Zayed University, UAE (e-mail: farkhund.iqbal@zu.ac.ae).

Benjamin C. M. Fung is with the School of Information Studies, McGill University, Canada (e-mail: ben.fung@mcgill.ca).

Patrick C. K. Hung and Laura Rafferty are with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Canada (e-mail: patrick.hung@uoit.ca, laura.rafferty@uoit.ca)

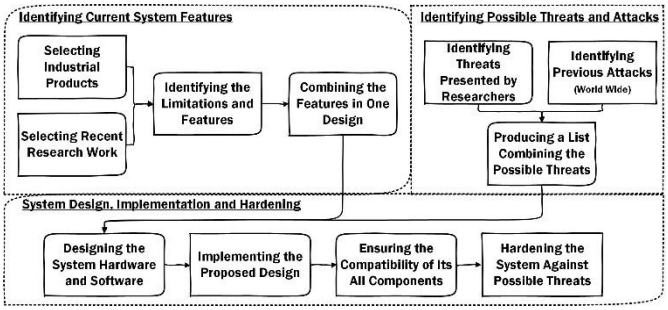


Fig. 1 Research structure and framework.

The rest of this paper is organized as follows. Section II presents a literature review. The main security threats to smart metering systems are discussed in Section III. The design and prototype implementation of the proposed system design is presented in Section IV. Next, the procedures used to harden the proposed system design and the rationale for them are elaborated in Section V. Finally, Section VI concludes the paper with future work.

II. Literature Review

A city could be considered smart if it uses the Information and Communication Technology (ICT) or Internet of things (IoT) to monitor and control its assets [33]. The assets that could be supported by the smart concept would be power grids, transportation systems, educational systems, and any governmental or private sector. In the United Arab Emirates (UAE), the adoption of smart city concept has recently received a lot of attention to include various services provided by different authorities including the municipality, health, police, roads, and transport, economic, electricity, water, etc. [34][35]. The smart grid is an essential part of smart cities as implementing it will result in increasing the throughput of the grid while reducing the energy consumption [36]. The traditional grid systems should have monitoring, analysis, control, and communication capabilities. The first attempt in bringing sustainability to the smart grid was introduced by Masdar City in Abu Dhabi that uses the combination of technology, architectural designs, and solar power to run a complete city while reducing the energy consumption and wasted resources [35]. The monitoring and control of power consumption on the consumer's side are achieved by smart meters. Smart meters normally involve real time measurements, power quality monitoring, and power outage notification [37]. The features and functionalities that are presented by smart meters exceeded the expectation to include advanced features. The recent proposed smart metering systems are discussed in the rest of this section and a summary of the discussion is presented in Table I.

Referring to the related research works in smart metering systems, Burunkaya and Pars [12] present a smart metering system that uses the Zigbee wireless technology to transfer the consumption data from multiple points to the server. A running Personal Computer (PC) was used as a server that receives the consumption data and displays them. The user can switch ON or OFF any device or point in the system remotely through the server. The proposed system provides a scheme for managing and transferring consumption data from multiple rooms to the server however it lacks in providing an interface to the user to interact and view the readings. The user needs a moderate level of computer experience to start serial monitoring software and initiate the connection with the XBee module connected to a computer to view the consumption data. Furthermore, the system is performed on the user side and does not introduce any means for moving the data from the user to utility company servers to perform automated way in recording the meter's readings.

Next, Karad et al. [46] present a smart meter that accepts recharge codes and verifies them with the power utility server to create a prepaid electricity system. The smart meter uses the Global System for the Mobile communication (GSM) cellular network to send the recharge card number alongside with the consumer identity to the power utility and hence the power utility reply to the smart meter whether the card number is valid or not with the associated recharged amount. The system based on Short Message Service (SMS) through the GSM cellular network that has been proven to be breakable by many researchers and accordingly the data can be sniffed and altered easily. It is recommended to use the latest cellular networks while implementing encryption and hashing techniques to ensure that the data will not be sniffed and altered.

Further, Khanji et al. [14] propose a system that measures the power consumption and transmit it through Bluetooth to an Android device that displays the data. The Orvibo WiFi Smart Socket and its free Android application were used through the proposed system to control one of the home appliances through WiFi. The proposed system presents a unique interface for the user that allows him to view and manage his power consumption, however, it has multiple issues. The main issue is the system dealing with multiple communication channels that are Bluetooth and Wi-Fi leading to extra load on the processors as well as more energy consumption. In this paper, the proposed system could be improved by providing a single interface that allows the user to view his consumption and manage the devices without the need to perform this task through different applications and different communication channels.

Then, Pawar et al. [13] present a smart metering system in which an Arduino UNO micro controller collects the power consumption data from all Arduino Yun microcontrollers that are connected to each household. Then the Arduino UNO micro controller uploads the consumption data to Temboo cloud and sends alerts and notifications to the user through email or SMS. The proposed system provides a convenient environment for sending the consumption details to the server, however, no security measures were considered as the data is uploaded without presenting any security measures like encryption. The proposed system eliminates the need for the power utility companies to send personnel to collect the meter consumption data manually, however, it only sends alerts and notifications when abnormal activities occurred to the Temboo cloud without presenting a local database for the measurements making the system not logging the consumption data when it the connection to the cloud is lost.

In addition, Preethi and Harish [47] introduce a smart

metering system that supports pre-paid and post-paid billing. The smart meter measures and calculates the consumption data and sends it wirelessly through Zigbee to a computer that is connected to a GSM modem. The computer sends the bills to the user and notifies the power utility company when detecting abnormal measurements through SMS. The system is based on GSM cellular network, which is an outdated communication system since it can be sniffed and altered easily by attackers. To improve the system, it is recommended to send periodic consumption data to the power utility company to analyze the measurements effectively while considering 4G Long Term Evolution (LTE) network or higher.

Moreover, Saikia et al. [45] propose a smart metering system with in home display that is based on GPRS. The system measures the voltage, current, power factor, and power consumptions and transfers them to a PC that acts as a home display unit as well as the power utility through General Packet Radio Services (GPRS). The home display unit is programmed by LabVIEW graphical programming language that needs a computer with an installed LabVIEW software to make it work, resulting in a huge load on the system. However, Saikia et al. did not consider any security measures and it is based on the GPRS that works with 2G and 3G cellular networks where the communication can be sniffed and altered through available industrial devices in the market. The system can be improved by reprogramming the home display unit in a programming language that makes the unit accessible from all smart devices types including mobile phones and tablets. The 4G LTE cellular network could be used as a base for the communication since it includes a strong encryption algorithm that has not been broken yet by attackers.

Lastly, Yaemprayoon et al. [11] propose a smart meter based on 32-bit PIC micro controller that measures the electric current to calculates the power. The consumption details are then saved in a Secure Digital (SD) card. The system presents a basic smart metering system that measures and stores the consumption details however it does not provide any feature of delivering the readings directly to the utility company. Accordingly, the system does not eliminate the need for assigning personnel to visit each house and collect the readings manually. Furthermore, having the readings on an SD card could be inconvenient for various types of users such as elderly customers as they may not have the sufficient experience with technology to extract the consumption data from the SD card.

TABLE I
SUMMARY OF THE LITERATURE REVIEW

Y	Authors	Objective	Contributions	Limitations
2017	Burunkaya and Pars [12]	To design and implement a smart metering system that measures consumption data from multiple points.	- The system connects multiple points wirelessly to the main server. - The main server can control the points and collect the consumption readings.	- The control and monitoring are based on command line interface. - The need for the power utility company to collect the consumption details manually is not eliminated.
2016	Karad et al. [46]	To design and implement a GSM based prepaid energy meter.	- The system measures the consumption data and sends it to the power utility servers to determine the cost. - It accepts recharge cards that are verified with power utility servers.	- The used GSM cellular network could be sniffed and altered easily as it is a not secure environment.
2016	Khanji et al. [14]	To design and implement Android-based measurement smart meter.	- The system measures the consumption data and displays it on an Android device. - It controls electronic devices wirelessly.	- The extra load on the system by using two different wireless channels. - No single interface for the system. - The need for the power utility company to collect the consumption details manually is not eliminated.
2016	Pawar et al. [13]	To design and implement a smart metering system that measures consumption data from multiple points and upload it to Temboo cloud.	- The system collects consumption measurements from multiple points. - It uploads the consumption data to cloud servers. - It sends SMS and email consumption notifications.	- No security measurements were undertaken. - Technical experience needed for the customer to view consumption data.
2016	Preethi and Harish [47]	To design and implement a smart energy meter that supports pre-paid and post-paid billing.	- The system measures and calculate the consumption data and send it wirelessly through Zigbee to a PC. - The PC sends the bills to the user and notify the power utility company when detecting abnormal measurements through SMS.	- No extensive consumption logging is maintained and stored. - The used GSM cellular network could be sniffed and altered easily as it is a not secure environment.
2016	Saikia et al. [45]	To design and implement a smart metering system based on LabVIEW and GPRS service.	- The system measures the consumption data and displays it on a PC. - It transmits the consumption data to the power utility company through GPRS.	- LabVIEW environment must be installed in the computer based display unit. - Not using the latest communication technology to ensure strong encryption.
2016	Yaemprayoon et al. [11]	To design and implement smart meter that saves consumption details on an SD card.	- The system digitizes the consumption measurements process. - It Generates and saving consumption logs.	- Reading the consumption logs require a certain level of experience. - The need for the power utility company to collect the consumption details manually is not eliminated.

III. SMART METER THREATS

Smart meters are exposed to different attacks that could be launched from different parties even from the consumer side [10]. Referring to Table II, it is noticeable that most of the meters perform power consumption measurements and deliver the consumption data to the power utility company. Some meters provide the consumers with in home display to allow them to view and track the real-time consumption, where the type of the data displayed varies from one type to another.

TABLE II
SUMMARIZED FEATURES OF THE INDUSTRIAL SMART METERS

Industrial Smart Meter Name	Main Features
Shark® 270 [5], OpenWay® [6]	- Provide automated consumption reading to the utility company. - No extensive interface for the client. - Simple meter with no advanced options. - Does not provide consumption readings to the utility company.
ScottishPower[7]	- Built-in screen as an interface for the client showing consumption details. - Simple consumption logging. - Provide automated consumption reading to the utility company.
Nexus 1500+[8]	- Built-in screen as an extensive interface for the client. - Advanced features and options (simple consumption logging, alarms). - Provide automated consumption reading to the utility company.
Shark® 200[9]	- Built-in screen as an interface for the client. - Web based interface for the client to read the consumption details.

- Advanced features (Extensive Data Logging, Alarm Email and Periodic Notification Email).

Having a device that is connected to the power grid network and located on the consumer side may encourage some of the consumers to perform illegal acts by either stealing energy or even hacking the main grid system through their home smart meter [4]. For example, Shuaib et al. [3] prove that two popular industrial smart meters, namely Shark 200 and Power Nexus 1500, were found to be vulnerable to different types of attacks. In their experiments, they performed Denial of Service (DoS) attacks on the smart meter through SYNflood tool and accordingly the smart meters were disconnected from the network. The same meters were found also to be vulnerable to Address Resolution Protocol (ARP) cache poisoning attack that can be performed by attackers to either reroute the traffic and sniff it or prevent the meter from communicating with the server. The main possible threat to think about is energy theft where malicious consumers attempt in all possible ways to use the electricity services without paying the bills. The identity spoofing attack could be used to either deny the service from another consumer or use the electricity services while making another consumer pay for it. In DoS, the attacker tends to deny the service from either other consumers or the power utility servers. More severe threats to smart meters include Sniffing and Traffic Analysis as well as malware spoofing, that is launched by professional attackers. The rest of this section lists these common threats to the smart energy meters.

A. Energy Theft

In this type of attack, consumers may use commercial devices or even develop their own to communicate with the smart grid and act as if they are legitimate smart energy meters to send fake usage data and reduce their bill [15]. This type of attack is common on the traditional power grid systems as well as the advanced smart metering system. For example, Czechowski and Kosek [23] classify the theft techniques into four main types including hidden connection in front of the meter, physical tampering with the terminals or bridging, physical tampering with an analog meter's mechanism and tampering with a digital meter's software. As a countermeasure to such attack, researchers propose various approaches. Next, Luan et al. [24] propose a detection approach based on multiple measuring stages to measure the delivered energy and compare the readings to detect if any tampering occurred. Further, Jiang et al. [25] propose a detection system that is based on machine learning and classification systems that study the behavior of the smart meters and predict whether there is tampering in the readings or not.

B. Identity Spoofing

In the same way, the attackers perform identity spoofing in computer network devices, they could perform a similar attack to spoof the identity of another smart meter that belongs to a legitimate user [16]. Doing so could transmit forged information to the power grid system resulting in a power cut or malfunction to both smart grid control system or the legitimate spoofed smart meter user. For example, Cimpanu [26] shows that even the most recently developed smart meters are still using the GSM network for transmitting their data which make the communication easy to sniff and manipulate as weak encryption techniques are implemented. Multiple devices that facilitate the process of intercepting and manipulating the GSM communication can be easily purchased and used by even beginners [27]. To limit such type of attacks, good encryption algorithms should be implemented alongside advanced authentication schemes and a full migration to the LTE infrastructure must be implemented to ensure that the security is maintained.

C. Denial of Service (DoS)

Attackers may tend to perform a denial of service attack on either the smart meter or smart grid. In both situations, a cut in the power will result producing huge losses [17]. In this attack, attackers send a huge number of requests to the smart meter or the smart grid causing them to malfunction. For example, Yi et al. [28] show how the traditional DoS attack through flooding the smart meter could create a drop down in the packet delivery rate to 34%. Furthermore, they present a new type of attack called puppet attack that could make the packet delivery rate reach 11%. Implementing good communication protocols and intrusion protection systems with packet filtering could limit such type of attacks.

D. Sniffing and Traffic Analysis

Attackers may get access to their neighborhood network through their smart meter and start sniffing the traffic produced by other smart meters. The sniffed traffic could be analyzed to generate a wide set of information that describes the power usage of a certain house [3]. The power usage information could identify what appliances are used and at what time the house is left without anyone staying in it. For example, Valli et al. [29] perform sniffing attacks to the wireless traffic on multiple frequencies ranges including 915 MHZ and 2.4 GHZ proving that good practices in implementing the communication are not implemented efficiently in recent industrial smart meters. A developer named BeMasher designs a system that is based on RTL-SDR dongles to detect the interval and standard consumption data of Itron C1sr smart meter in the 915MHz ISM band [30]. Good encryption algorithms could be implemented to limit the effect of such type of attacks.

E. Malware Spreading

Having a network that connects smart meters exposes them to the threat of being affected by malware spread [10]. The effect of malware on smart meters can be extremely dangerous as they may, for example, convert the smart grid to a botnet out of each zombie smart meter that is all controlled by an attacker. The attacker after compromising the smart grid could completely control it and perform his malicious acts easily

without having anyone stopping him. Mike Davis, a senior security consultant at the Seattle-based research company IOActive could demonstrate an attack on smart metering systems where he crafted a malware that replicated itself to other meters of the same type in a very short time to allow him to shut down the meters remotely [31]. To reduce the vulnerability of the smart meters to malware spreading, each smart meter must be designed in a way that accepts security updates periodically from the power company. A summary of the mentioned threats and their details with sample countermeasures proposed by researchers are shown in Table III.

TABLE III
SUMMARY OF SMART METER THREATS

Threat	Possible Attacks	Sample Countermeasures
Energy Theft	- Include hidden connection in front of the meter. - Physical tampering with the terminals or bridging. - Physical tampering with an analog meter's mechanism. - Tampering with a digital meter's software.	- Multiple measuring stages to measure the delivered energy and compare the readings [24]. - Predict the tampering based on the behavior of the smart meters [25].
Identity Spoofing	- Transmit a forged information to the power grid system. - Sniff and manipulate the communication.	- Implementing good encryption algorithms [26]. - Using advanced authentication schemes [27].
Denial of Service (DoS)	- Send a huge number of requests to the smart meter or the smart grid causing them to malfunction.	- Implementing good communication protocols [27]. - Using intrusion protection systems [54]. - Properly configuring packet filtering rules [28].
Sniffing and Traffic Analysis	- Identify what appliances of a certain house are used and at what time the house is left without anyone staying in it.	- Implementing good encryption algorithms [29].
Malware Spreading	- Convert the smart grid to a botnet. - Shut down the meters remotely.	- Implement periodic security updates [31].

IV. PROPOSED SYSTEM DESIGN & PROTOTYPE IMPLEMENTATION

Referring to Table I and II, a set of security procedures and techniques were selected as a baseline for developing our system. Our proposed system is designed from the scratch to have advanced metering features while keeping it secure. An extensive consumption of logs was considered in the system design to provide the user with detailed information allowing him to identify his consumption peak hours effectively. Significant energy-saving opportunities could be found by reading and analyzing the detailed consumption logs as the consumer will be able to manage and control his consumption efficiently when the consumer is receiving the detailed measurements [48]. Having such data of extensive consumption details could present a priceless feed to artificial intelligence and machine learning systems that could be used in the development of the smart grid including the enhancement of the load forecasting process [38]. The identification of whether an issue occurred at the customer's site and determine the proper way to resolving the issues [39]. The guidelines provided by the SANS Institute special publication 800-123 [40] for securing the devices were considered and implemented in the proposed system carefully to reduce the risks to its minimum levels. The secure File Transfer Protocol (sFTP) was used in transferring the consumption data from the smart meter to the power utility servers to ensure that the data is transferred privately and securely [41] [42]. In the proposed system, cryptography is also used for securing the communication between the customers and the Web portal of their smart meter as recommended by a SANS Whitepaper [43] through Transport Layer Security (TLS)/Secure Sockets Layer (SSL). Table IV shows a summary of the implemented countermeasures in the proposed system against common smart meters threats.

TABLE IV
IMPLEMENTED COUNTERMEASURES AGAINST COMMON THREATS

Threat	Implemented Countermeasures
Energy Theft	- Using electronic sensors that measure both live and neutral channels [49].
Identity Spoofing	- Forcing encrypted communication through Hyper Text Transfer Protocol Secure (HTTPS) [50].
Sniffing and Traffic Analysis	- Synchronizing the database through SSH File Transfer Protocol (sFTP) [51]. - Encrypting whole memory through VeraCrypt [52].
Denial of Service (DoS)	- Hardcoding server IP address. - Blocking big Internet Control Message Protocol (ICMP)/ broadcast requests [53]. - Installing SNORT intrusion protection system [54].
Malware Spreading	- Implementing periodic security updates.

The main features that are considered in the design are:

- Extensive consumption logging;
- Consumption data logging to the power utility securely through the Internet;
- Secure device that is not vulnerable to various attacks; and
- Full access to an advanced and secure Web portal on the meter.

Referring to Figure 2, the consumer should authenticate to log in, access the Web portal, and view the power consumption data. At the same time, all home appliances are working and their consumption data is recorded through the smart meter on its database that is synchronized periodically with the power utility servers. The power consumption measurements are done for the whole house at once as the sensors are connected to the main distribution board. The smart meter is recording and logging the consumption data in the database even if the consumer didn't request to view his consumption details. The database is synchronized with the power utility servers to generate the bill and identify the usage patterns. The consumer can view his consumption data from the local database by accessing the Web portal of the smart meter.

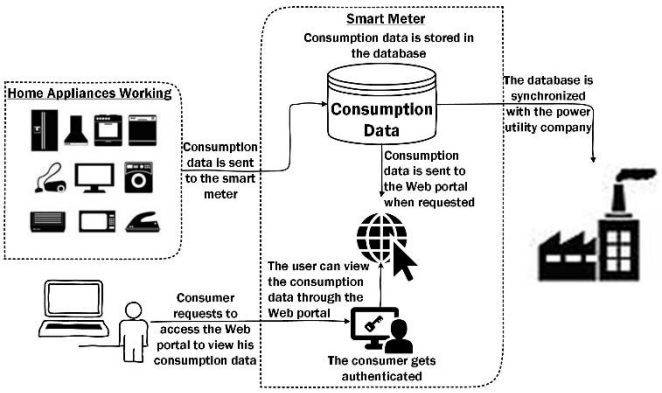


Fig. 2. A use case diagram for the proposed smart metering system

Figure 3 shows the prototype of the proposed system working under a test environment at the Cyber Forensics Laboratory in Zayed University, Abu Dhabi, UAE. The system consists of five main layers shown in Figure 4. The first two layers are based on selecting the proper hardware for the proposed system. The third layer identifies the process followed in recording the consumption details. The structure of the database and the means used to display the consumption details to the consumer are the main parts of the fourth layer. The last layer shows how the consumption details that are stored in the database are synchronized with the power utility servers. When relating our proposed smart metering system development layers to the Open Systems Interconnection Basic Reference Model (OSI) [59], the Electronic Sensors layer is basically a part of the Physical layer as it is responsible for measuring the analog values of the current and voltage and converting them to a digital signal that can be understood by the development board for further calculations and processing. The Development Board layer covers multiple layers of the OSI model including Physical, Data Link, Network, Transport, Session, and Presentation layers as it includes the hardware and software that is responsible for running the smart meter Linux operating system with a working network connection. The Application layer of the OSI model covers the Power Consumption Logging, Client-Side Web-based Portal, and logging to Power Utility layers.

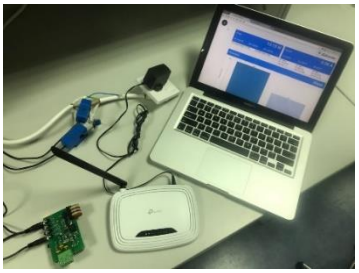


Fig. 3 A picture of the proposed smart metering system

5	**LOGGING TO POWER UTILITY**
4	**Client-Side Web-based Portal**
3	**Power Consumption Logging**
2	**Development Board**
1	**Electronic Sensors**

Fig. 4 Proposed smart metering system development layers

Layer 1: Electronic Sensors

The electronic sensors provide an essential part of any smart metering system as they are used to measure the current, voltage, and the power factor. Through the processing unit, multiple units are calculated. These units include the real power, reactive power, and apparent power.

The initial choice was to ACS712 [18] current sensor and its accuracy was tested with Protek 9902A [19] and GwINSTEK GFM-8145 [20] professional digital multimeters. A picture of the circuit used for this purpose connected to the project board is shown in Figure 5.

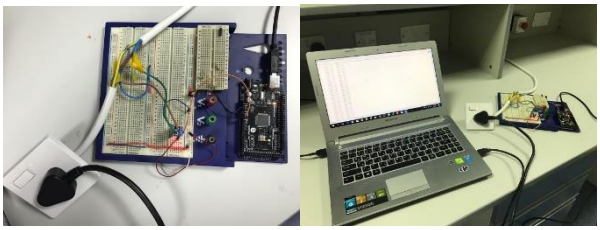


Fig. 5 Pictures of the testing environment of the ACS712 current sensor interfaced with Arduino microcontroller.

The readings were found to be not satisfying the needed accuracy level and accordingly the ACS712 sensor was replaced with SmartPi Sensors Board [21] shown in Figure 6, as it provides more accurate readings and makes the design extendable. The main features of the selected SmartPi sensors board are as follows:

- Measure currents up to 300A;
- Has 4x 3.5mm jack inputs for current transformers;
- Current transformers could be connected to the 3.5mm jack input;
- Measure three phase systems;
- Measure voltage in range of 400V on all phases; and
- Screw terminals for connecting the voltage measurement.

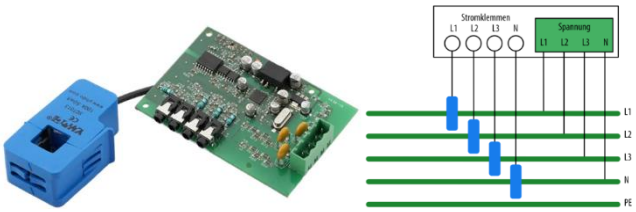


Fig. 6 On the left side, the SmartPi sensors board is shown while the right side shows the connections needed to measure the three-phase current. (Adapted from [18])

Layer 2: Development Board

The development board could be considered to be the motherboard of our proposed smart meter where the microprocessor, as well as all the sensors and the peripherals are located. Among different vendors such as Arduino, Intel Edison, and Mediatek Linkit, the Raspberry Pi3 Model B [22] development board shown in Figure 7 was selected to be programmed and configured to process and create our metering system. The main features of the board are as follows:

- A 1.2GHz 64-bit quad-core ARMv8 CPU;
- Supported by Linux OS;
- 802.11n Wireless LAN;
- 1GB RAM;
- Full HDMI port;

- Ethernet port;
- Combined 3.5mm audio jack and composite video;
- Micro SD card slot;
- 4-G data; and
- 4G USB Modem could be connected to it.

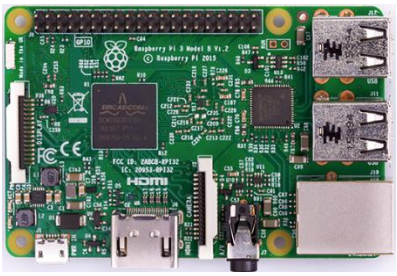


Fig. 7 A picture of the Raspberry Pi3 Model B development board (Adapted from [19])

Layer 3: Power Consumption Logging

An extensive power consumption logging process provides a convenient way for consumers as well as the power utility companies; but at the same time, the size of the logs must be considered carefully as to not consume a large amount of the memory for unneeded redundant data. In our proposed system, the logging process starts with an automated Python script that reads sensor values and keeps them in a temporary file. The temporary log file keeps rotating and replacing previous readings with the new ones. Each time an update occurs to the temporary log file, the previous readings are transferred to the MySQL database. Figure 8 shows the structure of each entry to the temporary log file that contains 15 parameters. The time stamp identifies the time the measurements were taken in relation to the system clock. In addition to the time stamp for each entry, the voltage, current, power, and power factor for each phase are logged as the proposed smart meter measures three phase systems.

Time Stamp		
Phase 1	**Phase 2**	**Phase 3**
- Voltage - Current - Power - Power Factor	- Voltage - Current - Power - Power Factor	- Voltage - Current - Power - Power Factor

Fig. 8 The structure of each entry in the temporary log file.

From these measurements, the power consumption details are calculated. The consumption records are used as a base for the instant monitoring by the Web portal as well as feeding the database. The logging is being performed in a secure way and data is designed to be not accessible by intruders or attackers.

Layer 4: Client-Side Web-based Portal

The main component of this layer is a MySQL Relational Database Management System (RDBMS) that includes multiple tables to cover hourly, daily, weekly, and monthly consumption details. The implemented MySQL database Entity Relationship Diagram (ERD) presented in Figure 9, shows five main tables in the database. The Consumer Details table includes the details that uniquely identify the consumer and his device. The other four tables include the details for hourly, daily, weekly, and monthly consumption data that are based on each other. This data gives a useful overview of power consumption patterns of the consumer.

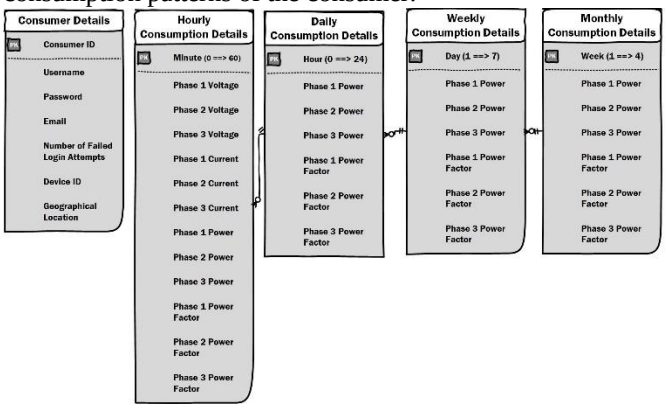


Fig. 9 Entity Relationship Diagram (ERD) for the structure of the implemented MySQL database

The whole database is encrypted and dumped periodically to the memory as well as the utility server. The user can access the PHP Web-based portal that displays live consumption measurements as well as the details from the database. Even if an attacker gets an access to the smart meter network, login credentials will be needed to log in to the portal.

Layer 5: logging to Power Utility

The utility server is Linux based as it provides a convenient environment that can be configured to perform the assigned tasks efficiently. Before logging to the power utility company, the database is checked to ensure that no alteration occurred. After dumping the smart meter database to a local directory, the dumped file is then uploaded securely to the utility server through an automated script that uses sFTP to transfer the file implementing encryption to maintain the integrity and confidentiality of the data.

The Unified Modeling Language (UML) diagram of the proposed system shown in Figure 10 has three main components; the initial stage where the readings are collected from the electronic current sensors by the Raspberry Pi micro controller and the power is calculated from the electronic current and voltage values. The obtained instant readings are saved in a file that its entries are replaced and updated periodically with the instant power consumption data. In the database management side, a trigger is initiated once the instant consumption data file is updated to retrieve the new records and preprocess them to make them ready to be inserted into the MySQL database. The MySQL database is synchronized periodically with the power utility servers through a Python script that transfers it through sFTP. When the user attempts to access the Web portal of the smart meter, the smart meter forces initiation of a secure encrypted communication through Hyper Text Transfer Protocol Secure (HTTPS). The user is then requested to authenticate his credentials to get access to the Web portal. The Web portal retrieves the instant consumption

data from the instant consumption data file and the previous records from the MySQL database and displays them to the user to have a good overview of the consumption details.

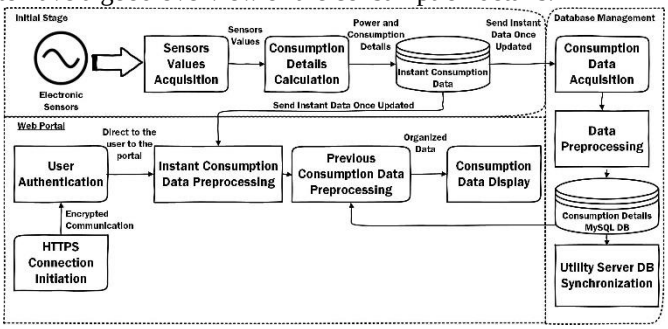


Fig. 10 Proposed smart metering system in UML

V. System Hardening

The main purpose of our proposed design is to prevent the previously mentioned attacks in Section III. Keeping in mind that attackers are always looking for weak points in any designed system, we need to keep implementing periodic security updates. The rest of this section presents the main points that have been performed in the Linux operating system of the smart meter to harden it and minimize the risks. The actions that have been implemented are based on the recommended techniques presented by Turnbull [44] for securing Linux files and file systems, connections, remote administration, and the proper means for firewalling the host. Using a development board that includes advanced hardware and software features implements performing the basic configurations to eliminate all the unneeded features to reduce the load on the system and more importantly to reduce the risk of getting the system hacked. To perform such task on the software side, the unnecessary tools and software packages, as well as the extra privileges and user accounts, could be removed. On the hardware side, the USB devices could be disabled [55]. Furthermore, the network could be secured by encrypting all the communication while blocking the unexpected traffic and implementing various network precaution techniques. To keep a track of the unexpected events and actions, auditing and logging must be implemented efficiently in the system. Figure 11 shows the actions considered both the smart metering system and the network as the system is connected to the Internet to deliver the consumption data to the power utility company. Further improvements could be added after performing penetration testing to the system.

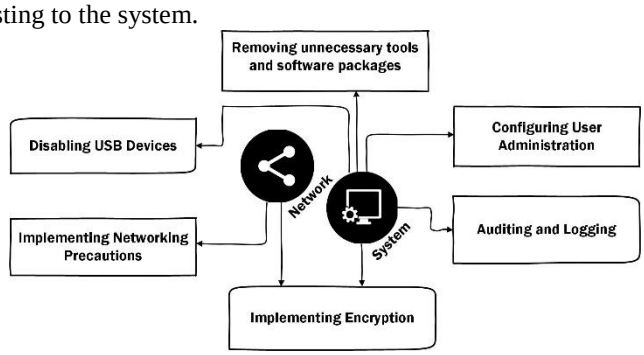


Fig. 11 The procedures and actions were taken in hardening the proposed design.

A. Removing unnecessary tools and software packages

Having extra unneeded software packages and services installed and running on the system will create an extra processing load that is not necessary [55]. Furthermore, having a package that is not updated or configured properly could create vulnerabilities in the system that can be used by attackers to hack the system [56]. In our proposed system, the list of all installed packages and available services are identified and out of these, only the necessary to run the smart metering system are kept. The disabled services and uninstalled packages are shown in Table V.

TABLE V
LIST OF REMOVED SOFTWARE PACKAGES AND DISABLED SERVICES FROM SMART METER OPERATING SYSTEM.

Removed Packages	Disabled Services
xserver-xorg-video-fbdev	anacron
xserver-xorg xinit	autofs
epiphany-browser	avahi-daemon
gstreamer1.0-libav	avahi-dnsconfd
omxplayer	bluetooth
raspberrypi-artwork	hidd
weston	cups
desktop-base	firstboot
netsurf-gtk	gpm
xpdf	haldaemon
xserver-xorg-video-fbturbo	hplip
minecraft-pi	kdump
python-minecraftpi	Kudzu
scratch	xfs

B. Configuring User Administration

In our proposed system, the user accounts are configured to be locked after three login failures. This action is important to ensure that attackers cannot perform a brute force attack to obtain the password for the users and log in through them [55] [44]. Another important action that has been considered is disabling the root login to make sure that even if the attackers obtained an access to the user account they will not be having full privileges and access to the system.

C. Implementing Encryption

Having the data or communication being encrypted ensures that it is of no use to the attackers if they gained access to it as it will be not in plain text [50] [51]. In the proposed system, the encryption has been implemented in two levels. The first level was the full disk encryption by VeraCrypt to encrypt the whole SD card memory and not allow the attackers to get any access to the system software and modify any part of it [52]. The other level was to encrypt the communication between the user and the smart meter portal by forcing the implementation of HTTPS for the Apache Web server that is used for the Web portal of the smart meter and sFTP for uploading the logs to the power utility server.

D.Auditing and Logging

Keeping a record of all the failed login attempts or abnormal power measurements could present useful information for the utility company to understand the actual reasons for a successful attack or even could be an early indicator of a possible one [57]. A script was written to obtain the useful logs about failed login attempts to the smart meter and the abnormal activities found in the portal and combine them into a single log file that is transferred to the utility server.

E. Implementing Networking Precautions

Implementing extra precautions to the network configurations reduces the risk of getting the meter being hacked or attacked. The IP address of the server is hard coded and big Internet Control Message Protocol (ICMP) / broadcast requests are blocked to eliminate the risk of getting the meter affected by DoS attacks [53]. SNORT intrusion protection system was installed as well to ensure that strong policies are applied on the system with the recent updates [54].

F. Disabling USB Devices

Raspberry Pi 3 development board provides four USB ports that can be used to connect any USB-based devices. To ensure that the attackers do not use these ports to launch their own malicious code, these ports were disabled [55].

In the proposed system, the power consumption measurements are done based on electronic current sensors that are not easy to manipulate like the traditional energy meters that are based on the disk speed of rotation in which bad consumers place a magnet on their meter to reduce the disk rotation thus reducing the bill. The risk of having bad consumers altering the smart meter software to reduce the consumption data is eliminated by implementing whole disk encryption to the smart meter memory. The system could be further improved by implementing machine learning models in the power utility server side that extract consumption features from the consumer's consumption data and determine whether tampering occurred or not and lunch alerts accordingly. Having the system constructed to be using the Internet protocol to transfer the consumption data makes the implementation of mature security standards and protocols easier than using industrial networks that are designed originally to be communicating on local environments within factories and not on a large scale like the case of smart energy meters that are distributed across the country. The transfer of consumption data and communication with the power utility server in the proposed system is done through sFTP that encrypts the whole communication, making it difficult to manipulate and spoof. The encrypted communication also makes sniffing and traffic analysis attacks not easy to perform as the data is transmitted not in plain text. To reduce the risk of getting the system affected by the DoS attacks, all the big ICMP broadcast requests were blocked since attackers tend to flood the victim by a huge number of PING requests making it unable to respond to the legitimate ones. The unusual traffic is detected and blocked by the installed SNORT intrusion protection system. Implementing packet filtering and strong policies to allow the expected type of traffic and block the unusual ones makes possibilities of spreading malware through the network very limited.

The implemented security precautions in the proposed system make it unique as most industrial smart meters are lacking to such features as shown in Table VI. However, even after implementing all the mentioned security precautions to limit the effect of the common attacks, new attacks will keep appearing making the need for periodic security updates essential.

TABLE VI
FEATURES COMPARISON OF OTHER SMART METERS WITH THE PROPOSED SYSTEM

Feature \ Smart Meter	Shark® 270 [5]	OpenWay® [6]	ScottishPower[7]	Nexus 1500+[8]	Shark® 200[9]	Bunnkaya and Pars [12]	Karad et al. [46]	Khanji et al. [14]	Pawar et al. [13]	Preethi and Harish [47]	Saikia et al. [45]	Yaemprayoon et al. [11]	Our Proposed System
Automated consumption logging to the utility company	√	√		√	√		√		√	√	√		√
Extensive details for the consumer				√	√	√		√	√		√	√	√
Accessible interface from smart devices			√		√			√			√		√
Implemented security measures													√
Supports pre-paid and post-paid billing							√			√			√
Compact design	√	√	√	√	√	√	√	√	√			√	√

VI. CONCLUSIONS

In this paper, the main threats to smart metering systems and its infrastructure were presented and analyzed. According to these threats and missing features of the industrial products as well as the proposed solutions by other researchers, a compact design for smart meter was introduced and a prototype was implemented to tackle almost all the known challenges. The security of the presented system was considered from scratch while having advanced metering features. The approach in hardening the system and making it more secure was elaborated in detail to act as a guideline for researchers and smart meter vendors in developing their new systems or improving their current products.

For future work, the database of the smart meter could be directly synchronized with the power utility servers to provide live measurements with an advanced logging system that can be accessed by the user through the internet anywhere in the world. More extensive logging and recording could be considered to provide a good feed for artificial intelligence systems to provide optimized solutions for the power utility companies. Furthermore, the current smart metering system could be integrated with a smart home to generate a system that can control and monitor the appliances through the smart meter portal. The security of the system can be investigated and

improved by applying well-studied attacks through penetration testing to identify the weak points in the system for improvement.

REFERENCES

[1] Monzon, A. (2015, May). Smart cities concept and challenges: Bases for the assessment of smart city projects. In International Conference on Smart Cities and Green ICT Systems (pp. 17-31). Springer International Publishing.

[2] Rawat, D. B., & Bajracharya, C. (2015, April). Cyber security for smart grid systems: Status, challenges, and perspectives. In SoutheastCon 2015 (pp. 1-6). IEEE.

[3] Shuaib, K., Trabelsi, Z., Abed-Hafez, M., Gaouda, A., & Alahmad, M. (2015). The resiliency of Smart Power Meters to Common Security Attacks. Procedia Computer Science, 52, pp. 145-152.

[4] Wurm, J., Hoang, K., Arias, O., Sadeghi, A. R., & Jin, Y. (2016, January). Security analysis on consumer and industrial iot devices. In Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific (pp. 519-524). IEEE.

[5] Shark® 270 Revenue Energy Meter. (n.d.). Retrieved May 29, 2017, from https://electroind.com/product-info/shark-270-energy-meter/

[6] Itron Access. (n.d.). Retrieved May 29, 2017, from https://www.itron.com/na/technology/product-services-catalog/products/2/a/f/openway-centron

[7] Smart Meters. (n.d.). Retrieved May 29, 2017, from https://www.scottishpower.co.uk/energy-efficiency/smart-meters/

[8] Nexus 1500 Next Generation Power Quality Revenue Meter. (n.d.). Retrieved May 29, 2017, from https://electroind.com/product-info/nexus-1500_plus-next-generation-power-quality-revenue-meter/

[9] Shark 200 Data Logging Power Meter/Transducer. (n.d.). Retrieved May 29, 2017, from https://electroind.com/product-info/shark-200-data-logging-power-metertransducer/

[10] Goel, S., & Hong, Y. (2015). Security Challenges in Smart Grid Implementation. In Smart Grid Security (pp. 1-39). Springer London.

[11] Yaemprayoon, S., Boonplian, V., & Srinonchat, J. (2016, June). Developing an innovation smart meter based on CS5490. In Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2016 13th International Conference on (pp. 1-4). IEEE.

[12] M. Burunkaya and T. Pars, "A smart meter design and implementation using ZigBee based Wireless Sensor Network in Smart Grid," 2017 4th International Conference on Electrical and Electronic Engineering (ICEEE), Ankara, 2017, pp. 158-162.

[13] Pawar, J. P., Amirthaganesh, S., & ArunKumar, S. (2016, November). Real time energy measurement using the smart meter. In Green Engineering and Technologies (IC-GET), 2016 Online International Conference on (pp. 1-5). IEEE.

[14] Khanji, S. I. R., Khattak, A. M., & Alfandi, O. (2016, July). Smart meter: Toward client centric energy efficient smartphone based solution. In Information, Intelligence, Systems & Applications (IISA), 2016 7th International Conference on (pp. 1-6). IEEE.

[15] Depuru, S. S. S. R., Wang, L., & Devabhaktuni, V. (2011). Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft. Energy Policy, 39(2), 1007-1015.

[16] He, D., Chen, C., Bu, J., Chan, S., Zhang, Y., & Guizani, M. (2012). Secure service provision in smart grid communications. IEEE Communications Magazine, 50(8),.

[17] McDaniel, P., & McLaughlin, S. (2009). Security and privacy challenges in the smart grid. IEEE Security & Privacy, 7(3), pp.53-61.

[18] ACS712: Fully Integrated, Hall-Effect-Based Linear Current Sensor IC with 2.1 kVRMS Voltage Isolation and a Low-Resistance Current Conductor. (n.d.). Retrieved May 29, 2017, from http://www.allegromicro.com/en/Products/Current-Sensor-ICs/Zero-To-Fifty-Amp-Integrated-Conductor-Sensor-ICs/ACS712.aspx

[19] Bench digital multimeter HC-9902A. (n.d.). Retrieved May 30, 2017, from www.lion.co.il/site/HvDest/hc9902a.pdf

[20] Digit Dual Measurement Multimeter, GDM-8145. (n.d.). Retrieved May 29, 2017, from https://www.gwinstek.com/en-US/products/Discontinued_Products/Discontinued_Meters_LCR/GDM-8145

[21] SmartPi - verwandeln Sie Ihren Raspberry Pi in einen Smart Meter. (n.d.). Retrieved May 29, 2017, from https://shop.enerserve.eu/smartpi/262/smartpi

[22] Raspberry Pi 3 Model B. (2016, February). Retrieved May 29, 2017, from https://www.raspberrypi.org/products/raspberry-pi-3-mode

[23] Czechowski, R., & Kosek, A. M. (2016, April). The most frequent energy theft techniques and hazards in present power energy consumption. In *Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG), Joint Workshop on (pp. 1-7).* IEEE. ISO 690

[24] Luan, W., Wang, G., Yu, Y., Lin, J., Zhang, W., & Liu, Q. (2015, November). Energy theft detection via integrated distribution state estimation based on AMI and SCADA measurements. In Electric Utility Deregulation and Restructuring and Power *Technologies (DRPT), 2015 5th International Conference on (pp. 751-756).* IEEE.

[25] Jiang, R., Lu, R., Wang, Y., Luo, J., Shen, C., & Shen, X. S. (2014). Energy-theft detection issues for advanced metering infrastructure in smart grid. Tsinghua Science and Technology, 19(2), pp. 105-120. ISO 690

[26] Cimpanu, C. (2017, January 05). Smart Meters Are Laughably Insecure, Are a Real Danger to Smart Homes. Retrieved July 08, 2017, from https://www.bleepingcomputer.com/news/security/smart-meters-are-laughably-insecure-are-a-real-danger-to-smart-homes/

[27] How to intercept mobile communications (calls and messages) easily without hacking. (2015, May 11). Retrieved July 08, 2017, from https://iicybersecurity.wordpress.com/2015/05/11/how-to-intercept-mobile-communications-calls-and-messages-easily-without-hacking/

[28] Yi, P., Zhu, T., Zhang, Q., Wu, Y., & Li, J. (2014, June). A denial of service attack in advanced metering infrastructure network. *In Communications (ICC), 2014 IEEE International Conference on (pp. 1029-1034). IEEE.*

[29] Valli, C., Woodward, A., Carpene, C., Hannay, P., Brand, M., Karvinen, R., & Holme, C. (2012). Eavesdropping on the smart grid. ISO 690 Page number??

[30] Connelly, A. (2014, February 25). Using SDR to Read Your Smart Meter. Retrieved July 09, 2017, from http://hackaday.com/2014/02/25/using-sdr-to-read-your-smart-meter/

[31] Naone, E. (2013, December 30). Meters for the Smart Grid. Retrieved July 09, 2017, from https://www.technologyreview.com/s/414820/meters-for-the-smart-grid/

[32] Zetter, K. (2016, March 03). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Retrieved July 15, 2017, from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[33] Cocchia, A. (2014). Smart and digital city: A systematic literature review. In *Smart city* (pp. 13-43). Springer International Publishing.

[34] Smart Dubai Current State (n.d.). Retrieved July 15, 2017, from http://www.smartdubai.ae/current_state.php

[35] United Arab Emirates Sustainable Cities. (n.d.). Retrieved July 15, 2017, from https://government.ae/en/information-and-services/environment-and-energy/sustainable-cities

[36] Smart Grid: What is it and why is it important? (n.d.). Retrieved July 15, 2017, from https://www.nema.org/Policy/Energy/Smartgrid/Pages/default.aspx

[37] Depuru, S. S. S. R., Wang, L., & Devabhaktuni, V. (2011). Smart meters for power grid: Challenges, issues, advantages and status. *Renewable and sustainable energy reviews*, *15*(6), 2736-2742.

[38] Zhao, H., & Tang, Z. (2016, June). The review of demand side management and load forecasting in smart grid. In *Intelligent Control and Automation (WCICA), 2016 12th World Congress on (pp. 625-629).* IEEE.

[39] Siryani, J., Tanju, B., & Eveleigh, T. (2017). A Machine Learning Decision-Support System Improves the Internet of Things' Smart Meter Operations. *IEEE Internet of Things Journal.?* Volume, Issue? Page number

[40] Kent, K., Jansen, W. A., & Tracy, M. (2008). *Guide to general server security recommendations of the National Institute of Standards and Technology*. Gaithersburg, Mar.: U.S. Dept. of Commerce, National Institute of Standards and Technology.

[41] Barker, E. B., & Roginsky, A. (2015). Transitions: *recommendation for transitioning the use of crytographic algorithms and key lengths.* Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology.

[42] Using SFTP in NIST 800-131a compliance mode. (2017, June 19). Retrieved July 19, 2017, from https://www.ibm.com/support/knowledgecenter/en/SS3JSW_5.2.0/com.ibm.help.nist_5242.doc/SI_5242_SFTP_nist_compliance.html

[43] Filinks, B., Northcutt, S., & Venafi (2015). *New Critical Security Controls Guidelines for SSL/TLS Management.* Gaithersburg, Mar.: U.S. Dept. of Commerce, National Institute of Standards and Technology.

[44] Turnbull, J. (2006). *Hardening Linux*. Apress.

[45] L. C. Saikia, H. Das, N. B. Dev Choudhury and T. Malakar, "GPRS enabled smart energy meter with in-home display and application of time of use pricing," *2016 IEEE Annual India Conference (INDICON)*, Bangalore, 2016, pp. 1-5.

[46] Karad, S., Kadam, Y., Jagtap, K., & Ghadge, P. (2016). GSM BASED PREPAID ENERGY METER. *International Journal of Advance Engineering and Research Development, 3(4).*Page number

[47] V. Preethi and G. Harish, "Design and implementation of smart energy meter," *2016 International Conference on Inventive Computation Technologies (ICICT)*, Coimbatore, 2016, pp. 1-5.

[48] Randy Barnett, American Trainco, Inc., for the Fluke Corp. | Jan 01, 2009. (2012, April 05). Saving Energy Through Load Balancing and Scheduling. Retrieved August 12, 2017, from http://www.ecmweb.com/power-quality/saving-energy-through-load-balancing-and-scheduling

[49] Paul Pickering | Sep 22, 2016. (2017, March 09). E-Meters Offer Multiple Ways to Combat Electricity Theft and Tampering. Retrieved August 12, 2017, from http://www.electronicdesign.com/meters/e-meters-offer-multiple-ways-combat-electricity-theft-and-tampering

[50] Chishkala, I. (2017, June 13). A Quick Guide to Securing Internet Traffic with HTTPS Encryption. Retrieved August 12, 2017, from https://www.upwork.com/hiring/development/a-quick-easy-guide-to-securing-your-site-with-https/

[51] SFTP – SSH Secure File Transfer Protocol. (2017, July 21). Retrieved August 12, 2017, from https://www.ssh.com/ssh/sftp/

[52] Campbell, A. (2016, November 14). 3 encryption tools for Linux that will keep your data safe. Retrieved August 12, 2017, from http://www.pcworld.com/article/3140023/linux/3-encryption-tools-for-linux-that-will-keep-your-data-safe.html

[53] R. (2010, February 12). Iptables: How to use the limits module. Retrieved August 12, 2017, from https://thelowedown.wordpress.com/2008/07/03/iptables-how-to-use-the-limits-module/

[54] Lincke, S. J., & Holland, A. (2007, October). Network security: Focus on security, skills, and stability. In *Frontiers In Education Conference-Global Engineering: Knowledge Without Borders, Opportunities Without Passports, 2007. FIE'07. 37th Annual* (pp. F1D-10). IEEE.

[55] Khawaja, G. (2016, November 26). Linux hardening: A 15-step checklist for a secure Linux server. Retrieved August 13, 2017, from http://www.computerworld.com/article/3144985/linux/linux-hardening-a-15-step-checklist-for-a-secure-linux-server.html

[56] Correa, D. (2017, March 23). Outdated software exposes millions of PC users to cyber-risks. Retrieved August 13, 2017, from https://www.scmagazineuk.com/outdated-software-exposes-millions-of-pc-users-to-cyber-risks/article/646030/

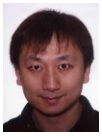
[57] Security Logs- Why are they so important? (2011, August 24). Retrieved August 13, 2017, from https://www.eventtracker.com/newsletters/why-are-workstation-security-logs-so-important/

[58] Kovacs, E. (2017, January 4). Smart Meters Pose Security Risks to Consumers, Utilities: Researcher. Retrieved August 14, 2017, from http://www.securityweek.com/smart-meters-pose-security-risks-consumers-utilities-researcher

[59] Alani, M. M. (2014). Guide to OSI and TCP/IP models. Berlin: Springer.

Musaab Hasan, received his B.Sc. in Electrical Engineering/ Communication (2012) from Ajman University, United Arab Emirates. Currently, he is working with the electrical engineering department of the same university as a teaching assistant. Mr. Hasan is also pursuing his M.S in Cyber Security at Zayed University, United Arab Emirates. He published various research papers in international journals and participated in several competitions and conferences. Mr. Hasan research interests are in cyber security, wireless communication, smart systems, and sensor networks.

Farkhund Iqbal Dr. Farkhund Iqbal holds the position of Associate Professor and Graduate Program Coordinator in the College of Technological Innovation. He holds a Master (2005) and a Ph.D. degree (2011) from Concordia University, Canada. He has served as a chair and TPC member of several IEEE/ACM conferences and is the reviewer of high rank journals. He is the member of several professional organization including ACM and IEEE Digital society. He has published more than 60 papers in high impact factor journals and conferences.



Patrick C. K Hung is a Professor at the Faculty of Business and Information Technology in University of Ontario Institute of Technology, Canada. He currently works with the College of Technological Innovation at Zayed University on several smart city and cybersecurity research projects in the United Arab Emirates. He is an Honorary International Chair Professor at National Taipei University of Technology in Taiwan and an Adjunct Professor at Nanjing University of Information Science & Technology in China. Patrick has been working with Boeing Research and Technology at Seattle on aviation services-related research with two U.S. patents on mobile network dynamic workflow system. Before that, he was a Research Scientist with Commonwealth Scientific and Industrial Research Organization in Australia as well as he worked as a software engineer in industry in North America. He is a founding member of the IEEE Technical Committee on Services Computing. He has Ph.D. and Master in Computer Science from Hong Kong University of Science and Technology, Master in Management Sciences from University of Waterloo, Canada and Bachelor in Computer Science from University of New South Wales, Australia. His research interests are in smart home security, Internet of Thing (IoT), and smart toys.

Benjamin C. M. Fung is the Canada Research Chair in Data Mining for Cybersecurity, an Associate Professor of Information Studies (SIS), an Associate Member of Computer Science (SoCS) at McGill University, a Co-curator of Cybersecurity in the World Economic Forum (WEF), and a Research Scientist in the National Cyber-Forensics and Training Alliance Canada (NCFTA Canada). Collaborating closely with the national defense, law enforcement, transportation, and healthcare sectors, he has over 100 refereed publications that span across the research forums of data mining, privacy protection, cyber forensics, services computing, and building engineering. His data mining works in crime investigation and authorship analysis have been reported by media worldwide. Before joining McGill, he was an Assistant/Associate Professor at Concordia University, and a system software developer at SAP Business Objects in Canada. Dr. Fung is a licensed professional engineer in software engineering. See his research website http://dmas.lab.mcgill.ca/fung for more information.

Laura Rafferty, received her B.IT. in Networking and IT Security and M.Sc in Computer Science from University of Ontario Institute of Technology (UOIT), Canada. Currently, she is a Ph.D. candidate in Computer Science at UOIT. Further, she is working at the security team and she is an Internet of Thing (IoT) committee member in security at CIBC bank at Toronto, Canada. She has published research papers in smart toys privacy and IoT security at various book, journal and conference. Her research interests are in smart home security, Internet of Thing (IoT), and smart toys.