Secure Data Sharing and Analysis in Cloud-Based Energy Management Systems

Eirini Anthi[1], Amir Javed[1], Omer Rana[1], and George Theodorakopoulos[1]

School of Computer Science & Informatics, Cardiff University, UK
javeda7@cardiff.ac.uk

Abstract. Analysing data acquired from one or more buildings (through specialist sensors, energy generation capability such as PV panels or smart meters) via a cloud-based Local Energy Management System (LEMS) is increasingly gaining in popularity. In a LEMS, various smart devices within a building are monitored and/or controlled to either investigate energy usage trends within a building, or to investigate mechanisms to reduce total energy demand. However, whenever we are connecting externally monitored/controlled smart devices there are security and privacy concerns. We describe the architecture and components of a LEMS and provide a survey of security and privacy concerns associated with data acquisition and control within a LEMS. Our scenarios specifically focus on the integration of Electric Vehicles (EV) and Energy Storage Units (ESU) at the building premises, to identify how EVs/ESUs can be used to store energy and reduce the electricity costs of the building. We review security strategies and identify potential security attacks that could be carried out on such a system, while exploring vulnerable points in the system. Additionally, we will systematically categorize each vulnerability and look at potential attacks exploiting that vulnerability for LEMS. Finally, we will evaluate current counter measures used against these attacks and suggest possible mitigation strategies.

Key words: Internet of Things, Security and Privacy, Smart Grids

1 Introduction

Smart grids can be defined as a network of intelligent entities that are capable of bidirectional communication and can autonomously operate and interact with each other to deliver power to the end users. Over the years smart grids have been used to address the high energy consumption of commercial building or set of buildings. As it was reported by the United Nations Environment Program that residential and commercial buildings consume approximately 60% of the worlds electricity. In addition to using 40% of global energy, 25% of global water, and 40% of global resources. Interestingly, because of the high energy consumption, buildings are also one of the major contributors to greenhouse gas production [38, 22], but also offer the greatest potential for achieving significant greenhouse gas emission reductions, with numbers projected to increase [34, 51]. For these reasons improving energy efficiency of buildings has received a lot of attention globally [52]. Smart grids based energy management systems have been used to reduce the energy demand of a building or set of buildings however, these systems have their own challenges. Such as they have central point of failure and scalability issues due to limited memory [3]. Researchers over the years have suggested a cloud based energy management system that is not only scalable, it does not have a single point of failure and because of its on demand allocation of resources, it uses only the energy required for the energy management system.

Keeping these challenges in mind and to overcome them, a cloud based demand response system was proposed that introduced data centric communication and topic based communication models [20]. Their model was based on a master and slave architecture, in which the smart meters and energy management system at home acted as slave where as the utility acted as masters. The authors advocated that a reliable and scalable energy management system can be built using their model. Energy pricing is considered to be one of the relevant factor as the energy consumption cost is determined by it. Taking this into consideration, an energy management system was built by considering the energy pricing to be dynamic [23]. While building this model, the authors considered the peak demand of the building and incorporated the dynamic pricing while handling customer requests. While designing a cloud based energy management system [39] proposed an architecture for control, storage, power management and resource allocation of micro-grids and to integrate cloud based application for micro-grids with external one. The bigger and distributed the smart grid infrastructure becomes, the more difficult it is to analyse real time data from smart meters.

Yang et al. [53] suggested that a cloud based system is most appropriate to handle the analysis of real-time energy data from smart meters. In another approach, power monitoring and early warning system facilities were provided using a cloud platform [17]. A mobile agent architecture for cloud based energy management system was proposed to handle customer request more efficiently [46]. Focusing on the energy demand a dynamic cloud based demand response model was proposed to periodically forecast demand and by dynamically managing available resources to reduce the peak demand [42].

The shift of micro-grid based energy management system to cloud based energy management system does overcome many challenges faced by conventional smart grid based energy management system. However, whenever we expose a model to the internet, security and privacy concerns are raised. In this paper we address these issues for the cloud based energy management system and particularly for the Internet of Things (IoT) devices that are integrated into it. The analysis is done by a live example of a cloud based Local Energy Management System (LEMS) and later extended to general cloud based energy management system. The LEMS is developed and deployed on cloud (i) to flatten the demand profile of the building facility and reduce its peak, based on analysis that can be carried out at the building or in its vicinity (rather than at a data center); (ii) to enable the participation of the building manager in the grid balancing services market through demand side management and response.

1.1 Contribution

In this paper we describe the architecture of a Cloud-based Energy Management System (LEMS), that is developed to reduce the energy demand of a commercial building or set of buildings in the United Kingdom. We will further give an overview of the LEMS operation, using which a building manager can reduce the energy cost using intelligent devices such as smart chargers, EVs/ESUs present at the building site. We then provide a systematic overview of the major cyber attacks against LEMS and the associated data capture devices involved. The main aims of this paper are:

– Give an architectural overview of LEMS and its operations.
– Identify cyber attacks LEMS.
– Provide an overview of counter measure/mitigation strategies for these attacks and identify any research gaps.

The structure of the paper is as follows: Section 2 discusses the LEMS architecture and give an overview of its operations. Section 3 gives an overview of attacks identified for cloud based energy management system and presents current counter measures. Section 4 concludes the paper.

2 Cloud based Local Energy Management Systems

In order to give a systematic security overview of a cloud based energy management system we deployed a cloud based local energy system and used it as a case study to address the security concerns. The proposed energy management system can be divided into three parts: a) the IoT devices that are present at the edge of the network, b) the main LEMS algorithm deployed in the cloud, and c) the GUI which is used to control the LEMS. The architecture of Local energy Management System (LEMS) is presented in Fig. 1. The main objective of LEMS is to manage the building demand by using various IoT devices at building premises by sending power set points through a Gateway to Electric Vehicle (EV) chargers and Energy Storage Units (ESUs).

IoT devices at the network edge

The cloud based energy management system and our LEMS, depend on various smart devices such as: smart meters, chargers, electric vehicles, energy storage units, to gather information from the environment/buildings and to control the energy flow. Smart meters measure the energy consumption of the commercial building at a 15 minute interval. The chargers are capable to charge but also discharge an electric vehicle, in order to efficiently manage the energy demand of the connected buildings. The electric vehicles and energy storage unites reserve energy, that can be supplied to the buildings whenever is needed to reduce the energy cost or demand.

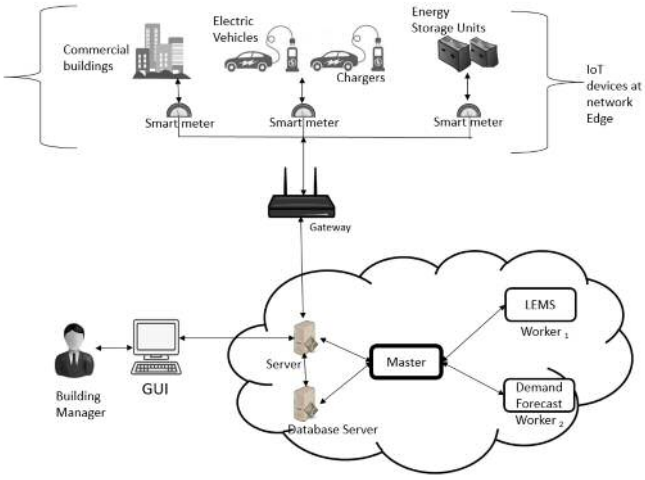


Fig. 1: Architecture of Cloud based Local Energy Management System

The LEMS Algorithm and the GUI

The heart of the LEMS consists of a demand forecasting tool and a scheduling algorithm. The rationale to add a forecasting tool, was to be able to predict in advance what the building's energy demand, so that a schedule can be created to reduce this expected demand. The demand forecast tool estimates the electricity demand of the building for a particular time period. The demand forecasting tool made use of a neural network (from the Weka toolkit [32]) using historical data (collected from actual building use) and weather data within the proximity of the building.

The LEMS scheduling algorithm operates in timesteps during which the system is considered static (changes are only discovered at the end of the timestep). A time step is defined as a time interval after which the LEMS read the data from each components such as building, EVs/ESUs, etc. For our case study we have kept the timestep duration to be 15 minutes. It was concluded that this timestep duration is an acceptable trade-off between a dynamic (semi-real time) and a reliable operation that allows the frequent capture of the building conditions and minimizes the risk of communication lags. Data about EVs located at the building, such as their battery capacity, state of charge (SoC), expected disconnection times, charging/discharging power rate, charging/discharging schedule and available discharge capacity, is requested from the EV charging stations upon the connection of every EV. Information regarding the available capacity, state of charge (SoC), charging/discharging power rate and charging/discharging schedule is requested from every ESU. This information is stored in a database, and is accessed from the LEMS on a regular basis (every 15 minutes) in order to define the future power set points for the chargers.

The LEMS is deployed on the CometCloud [5] system. CometCloud enables federation between heterogeneous computing platforms that can support complete LEMS work, such as a local computational cluster with a public cloud (such as Amazon AWS). There are two main components in CometCloud: a *master* and (potentially multiple) the *worker* node(s). In its software architecture, CometCloud comprises mainly three layers: the programming layer, an automatic management layer and a federation or infrastructure layer. The programming layer defines the task that needs to be executed, the set of dependencies between tasks that enables a user to define the number of resources that are available along with any constraints on the usage of those resources. Each task in this instance is associated with the types of LEMS operation supported, or whether a demand forecast needs to be carried out. In the automatic management layer the policy and objectives are specified by the user that help in allocating the resource to carry out the task. In addition to allocation of resources, this layer also keeps a track of all task that are generated for workers are executed or not [6]. In the federation layer a look-up system is built so that content locality is maintained and a search can be carried out using wildcards [30]. Furthermore, a "CometSpace" is defined that can be accessed by all resources in the federation [26]. Essentially, CometCloud uses this physically distributed, but logically shared, tuple space to share tasks between different resources that are included in a resource federation. The main task of the master node is

to prepare a task that is to be executed and give information about the data required to process the task. The second component is the worker, which receives request from the master, executes the job and sends the results to the place specified by the master. In our framework there are two workers – one that will be running the LEMS algorithm that will generate the schedule and the second that will forecast energy demand for the next day, to generate the charging and discharging of the electric vehicles.

There are two cloud-hosted servers that receive requests from a graphical user interface, and based on the requests call the appropriate function via the master. The second server manages a database which contains information about building data, EVs and weather attributes around the building. The database is used to store historic data about power consumption, energy pricing, and more, for each building. Information regarding the weather is also used to forecast (energy) the energy demand for the next day. There is an intermediary gateway, which intercepts all signals from the cloud server and forwards the requests to the EVs to either charge or discharge.

The energy management system is designed for various purposes such as to reduce demand, reduce energy cost etc. The LEMS that we had developed maximizes its utility to the building manager by adjusting its operational target (objective) according to the system status and condition. Furthermore, it was designed to create two scheduling algorithms for the management of the EVs and the ESUs, namely Peak Shaving Schedule and Demand Response Schedule respectively. Each algorithm serves one objective and the LEMS shifts from one scheduling strategy to another depending on the objective of the building manager. The peak shaving algorithm aims to flatten the aggregate demand profile of the building facility. This is achieved by filling the valleys and shaving the peaks of the demand profile using the controllable loads (EVs, ESUs) of the building facility. The LEMS calculates the charging/ discharging schedules of the EVs and ESUs, and sends them the corresponding power set points at the beginning of every timestep. For the demand response algorithm a demand response signal is send by the the building manager to either reduce or increase its aggregate demand in the next time step (of 15 minutes). Triggered by the arrival of such a request, the LEMS overrides the charging/discharging schedules of the available controllable assets.

3 Security Concerns of Cloud based Energy Management System - LEMS as case study

Energy systems designed to manage the energy consumption of commercial buildings have certain security challenges to combat. These include the system availability at all times and ensuring that the power is not lost or stolen. As these systems are migrating regularly to the cloud, their complexity increases. Whilst designing such systems, it is important to employ various security mechanisms to defend them against cyber attacks. However, regardless of that, there will always be vulnerabilities ready to be exploited by cyber criminals.

Researchers in the past have suggested many strategies to protect these cloud based energy management systems. Emphasizing on the cloud security, a client-server based model was proposed by Wang et al. [49]. The main idea of this model is that all the data processing and important tasks would be performed on a secure cloud platform, and the client would only be responsible for collecting data. Simman et al. [43] looked at security risks and concerns for public, private and hybrid cloud platforms that can be used to deploy the energy management system. The authors concluded that private cloud is more suitable for deploying energy management system as they are less prone to malware and are easily containable. However hosting and maintaining a private cloud is more expensive than public cloud. Ugale et al. [47] focused on the security of the data stored on cloud by proposing a distributed verification protocol. Maheshwari et al. [28] proposed that by using public key infrastructure one can mitigate issues relating to fault tolerance and can detect any intrusion in the system. While most research has been on the security of the cloud, Wen et al. [50] focused on the security of the smart grids that are integral part of the energy management system. The authors proposed that by encrypting smart meter data on the cloud, its privacy is being preserved, as only authorised people can access it. Although the research that has already been conducted to secure cloud and data stored is important, it is also significant to investigate the security of other components that are integral parts of the energy management system. The security concerns that are addressed are looking at the kind of attacks that are used to bring down a cloud based energy management system.

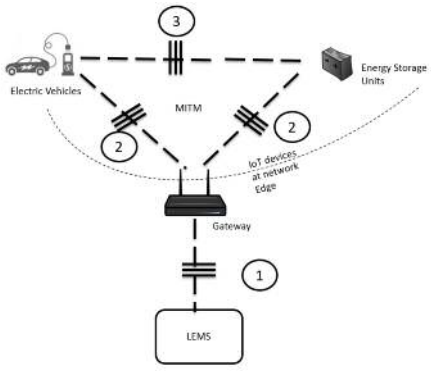
The term Internet of Things (IoT) is used to describe a structure of interconnected devices, which provides automation and various other functionalities [1]. A cloud based energy management system and our LEMS depends on various smart objects such as: smart meters, chargers, electric vehicles, etc., to gather information from the environ-

ment/buildings and to control the energy flow. Although these devices provide great opportunities in the concept of Smart Grids, they come with tremendous security risks [18, 57, 45].

The architectural structure of IoT can be divided into three key layers [10]. The Perception Layer, Network Layer, and Middle-ware layer. The Perception Layer consists of different kinds of data sensors such as RFID. The Network Layer refers to the data transmission process, where information gathered from the perception layer gets transferred to an information processing system via communication networks, such as: the Internet, Mobile Network, etc [56]. Finally the Middle-ware layer consists of information processing systems such as cloud storage infrastructures. Each one of these layers presents its own security issues to combat.

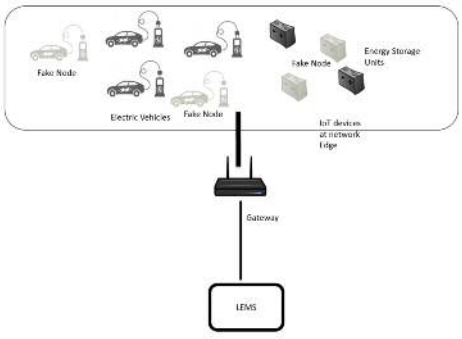
While evaluating the architecture of a cloud based energy management system for vulnerabilities, we have identified a number of cyber attacks that can bring down the system. We will focus on discussing in detail the attacks targeting the Network Layer of the IoT system associated with the LEMS. Finally, we will present the current counter measures against these attacks and also suggest the most suitable strategies to defend our energy management system.

3.1 Data Leakage



0.5

Fig. 2: An attacker can eavesdrop on on the communication channels between 1) the gateway and the LEMS, 2) the gateway and the IoT system, and 3) among the IoT devices.



0.5

Fig. 3: An attacker forges a number of identities to act as legal nodes (impersonate EV/ESUs) on the system, so that its energy consumption levels will be increased.

Fig. 4: Architecture of Predictive Model

As one of the key features of a smart grid based energy management system is bidirectional communication, an attacker could eavesdrop on information from the communication channels between: a) the gateway and LEMS, b) the

gateway and the IoT system, and c) among the IoT devices (i.e. between the smart charger and the electric vehicle) [10] as per Figure 2. If the Secure Sockets Layer (SSL)/ Transport Layer Security (TLS) protocol [12, 7] is not employed and therefore the data that gets transmitted is not encrypted, an unauthorized party could simply intercept it by performing passive network sniffing on the operating channel [2, 19].

If the SSL/TLS protocol is employed, and therefore the transmitted data is encrypted, an eavesdropping attacker can observe it to identify traffic patterns and hence gain information about the functionality of the system. For example, the smart energy storage units that are used in the LEMS send information to the gateway about their energy status every 15 minutes. The adversary could use this information to identify when and how the energy management system is going to adjust the energy requirements of the buildings and therefore could alter the scheduling algorithm sent to the energy storage units. Once the scheduling algorithm is altered, the cyber criminal can create a situation where the ESU's and EV's are charging at peak hours resulting in increasing the energy demand at these hours. This will increase the energy demand and cost for the company and defeat the purpose of deploying an energy management system.

Additionally, an attacker can perform a Man-In-The-Middle (MITM) attack. With this attack the original connection between the two parties gets split into two new ones: one connection between the first party/device and the attacker and another one between the attacker and the second party/device. When the original connection is finally compromised, the attacker is able to act as a proxy and therefore read, insert, and modify data in the intercepted communication [33].

In cases where the attacker has managed to compromise the communication channels, using any of the above discussed methods, they could gain access to important information such as: IDs from the electrical vehicles, electrical signals/pulse from the batteries, meter readings etc. This could significantly impact the energy management functionality of the LEMS and the energy cost. For instance, if an unauthorised party interfered (spoofed, manipulated, inserted, or deleted) with the unique IDs of the batteries of the electrical vehicles, then the LEMS would receive false information from the gateway and it would not be able to adjust correctly the building's energy demand.

To defend the energy management system, the SSL/TLS protocols should always be used to establish a secure channel for communication among all the parties/devices in the LEMS. Nevertheless, this protocol is not enough to prevent MITM attacks. Consequently, techniques such as certificate pinning [16], should also be employed to authenticate the devices on the grid. This ensures that each device checks the servers certificate against a known copy stored in its firmware [11]. However, although this is an efficient way of preventing MITM attacks it is not completely immune, as an adversary could disable the certificate pinning procedure, and manage to intercept the communication [31]. As an alternative to SSL/TLS, managed certificate whitelisting was recently proposed [9] to authenticate devices, specifically in energy automation systems. Even though this approach appears to be promising, its security aspects haven't been fully explored. Finally, to protect against traffic analysis, [27] proposes a re-encryption algorithm that can be used to randomise the transmitted cipher text, without affecting the decryption process. This prevents the attacker from linking in and out data by comparing the transmitted packets.

3.2 Spoofing

Sybil attack is a type of spoofing attack in which IoT devices on the LEMS are particularly vulnerable [55]. During such attacks, attackers can manipulate fake identities to compromise the effectiveness of the IoT as per Figure 3. For instance, in the energy management system, such an attack could forge a massive number of identities to act as legal nodes and request more energy from the LEMS. This could severely affect the energy cost and latency of the system.

Various methods to detect and defend against Sybil attacks have already been implemented and can be employed on the LEMS. For instance, SVELTE, is a novel Intrusion Detection System designed specifically for IoT devices, which is inherently protected against Sybil attacks [**?**]. Alternatively, Zhang et al. [55] discuss some cryptography-based schemes MSD (crypto-MSD), that can also defend against these attacks. Finally, the use of a unique shared symmetric key for each node on the system with the base station/gateway is another way to defend against it [58, 48, 41].

3.3 Disruption of Service (DoS/DDoS)

Denial of Service attacks (DoS) are the most common kind of attacks that can occur in a network and can severely impact the internet of things [45]. These reduce, interrupt, or completely eliminate the network's communications,

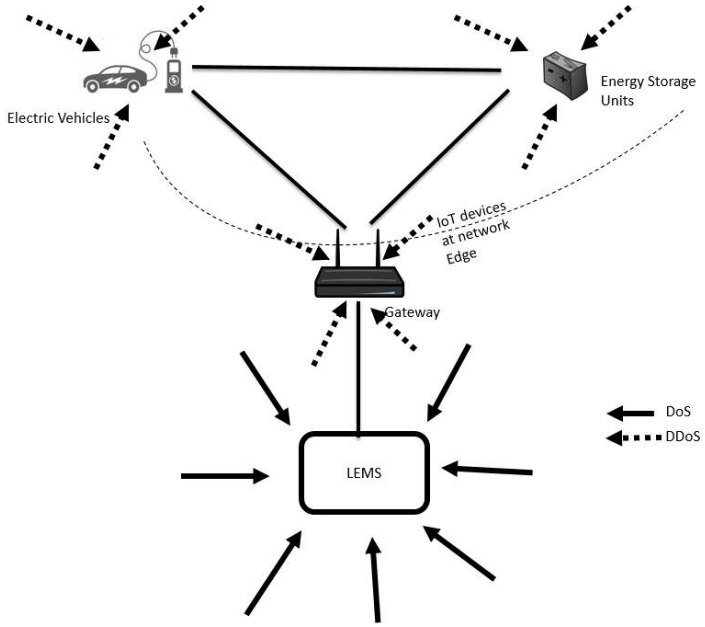


Fig. 5: A denial of service attack (DoS) could target the LEMS, or a distributed denial of service attack (DDoS) could also target the IoT system.

and range from jamming to more sophisticated attacks [35]. In any network and specifically in an energy management system, *device availability* is crucial. As DoS attacks target to destroy the availability of communication among them, they can have serious reverberations on the system [45].

DoS attacks can be initialised remotely and they are very hard to detect before the network/service becomes unavailable. This is why they are considered to be one of the most serious networking threats [19, 45]. DoS attacks can also evolve to distributed DoS (DDoS) attacks and in this case the attacker could take down the LEMS, as per Figure 5.

Given the way our management energy system is designed, we can have two scenarios of DoS/DDoS attacks. A DoS attack could target the LEMS system and a DDoS attack could also target the IoT devices on the grid. In the first case, the communication between the LEMS and the IoT would be lost and there would be no way to control the energy flow on the energy management system. The second scenario is more severe and therefore we will describe it in more depth.

Consider that an attacker identifies an exploitable vulnerability in the smart energy storage units used in the energy management system, which would allow them to charge and discharge them whenever they want. They can then create an exploit that will help them locate and take control of all these vulnerable devices on the LEMS (bot herder)[8]. At this point the adversary would be able to constantly discharge the batteries, resulting in wasting huge amounts of energy and a possible blackout of the system. As our energy management system is connected to the National Grid, the hacker could potentially take control of it too. As a result , this would lead to serious financial losses and not only. A recent study by Dlamini et al.[8] showed that this scenario could also result in loss of lives.

Although various mechanisms against DoS attacks have been proposed, none of them can provide full protection against them all. Raymond et al. [40], discusses currently used protection methods against DoS in Wireless Sensor Networks. Moreover, Garcia et al. [13, 14] present various DoS countermeasures such as: DTLS, IKEv2, HIP, and Diet HIP, for IP-based Internet of Things. Finally [19] proposes a DoS detection architecture for 6LoWPAN network with great potential. It is necessary to underline that due to the severity of DoS attacks, there is a need to research better preventive measures and defensive mechanisms [29].

3.4 Energy Bleeding

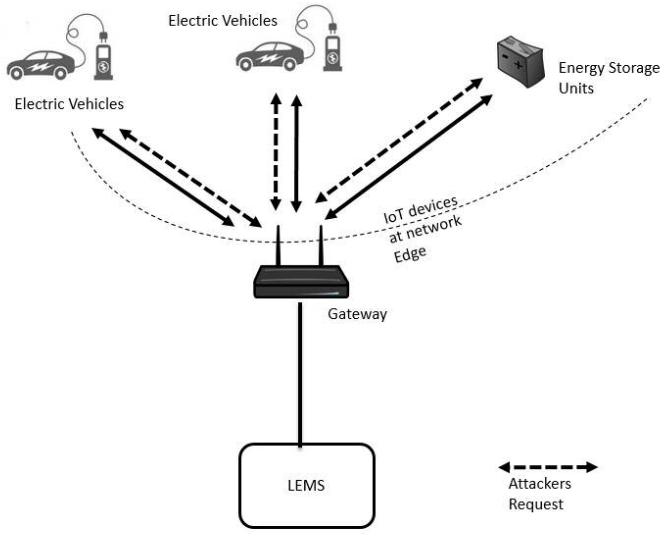


Fig. 6: An attacker will keep sending requests to the devices, using either the Barrage or Sleep Deprivation attack, in order to prevent them from going into a power-saving mode.

In sensor networks like the cloud based energy management system, the ability of the devices to enter power-saving modes (e.g various sleep and hibernation modes) is important to preserve the network's longevity, the lifetime of these devices, and reduce the overall power consumption [36, 37, 15]. In this section two major attacks that target this functionality of the devices will be discussed: sleep deprivation and barrage attack. Specifically, an attacker can use them to forbid these devices from going into power-saving mode by continually sending traffic to them and hence exhausting their battery resources [21], as per Figure 6. These are also known as *sleep deprivation torture attacks* [44]. Both of them, if used against the LEMS, could cause severe energy and therefore financial losses.

During the barrage attack the targeted device is being bombarded with requests that seem to be legitimate. The goal is to waste the device's limited power supply by preventing it from going into sleep mode and making it perform complex energy demanding operations. In sleep deprivation attack, malicious nodes on the network, send requests to the victim device only as often as necessary to keep it switched on. Although the goal of this attack is the same as the barrage attack, the sleep deprivation attack does not make the target nodes perform energy intense operations [36]. Barrage attack has been proven to exhaust faster the battery resources of the targeted nodes [36], but at the same time it is very easy to detect as opposed to sleep deprivation attack. For this reason we consider sleep deprivation to be more a more serious threat [21].

Pirreti et al. [36] showed that sleep deprivation attack can impact severely networks like the LEMS. They demonstrated that if an attacker manages to compromise as few as 20 devices on a 400 node network, they will be able to double its power consumption. Additionally, they showed that a single malicious node can attack approximately 150 devices at the same time. Therefore this attack can significantly affect the energy consumption levels of the system.

To protect the energy management system from sleep deprivation attack, we can use any of the currently implemented mechanisms. For instance, Pirretti et al. [36], extensively compares and evaluates three different defence schemes against sleep deprivation attack that can be applied in sensor networks. These include the random vote scheme, the round robin scheme, and the hash-based scheme. Finally, another recent study [4] proposes a framework based on distributed collaborative mechanism, that efficiently detects sleep deprivation torture.

3.5 Insecure Gateways

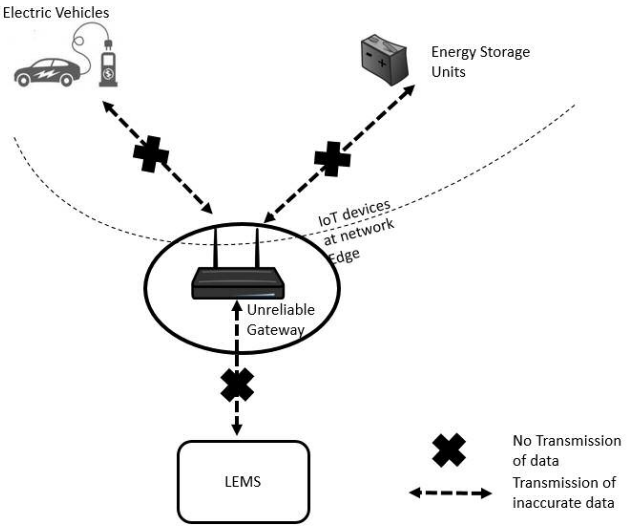


Fig. 7: In this case the vulnerable point of the system is the gateway. Data may get transmitted inaccurately or not transmitted at all.

One of the most basic components of our energy management system is the gateway, which is responsible for transmitting information from the IoT devices to the LEMS and vice versa. As the LEMS adjusts the energy flow on the system according to the information it receives from the gateway, we need to examine its reliability by exploring possible issues associated with it and current solutions.

The gateway can be considered to be untrustworthy if it does not transmit any data to the LEMS/IoT, or if it transmits it inaccurately [25], as per Figure 7. Reasons why a gateway could be faulty consist of complications to wireless media, software issues and hardware defects. This could lead to increase in communication delays, waste of bandwith, increased power consumption, data loss, and communication failures on the system [25, 54]. Various network attacks such as the ones described in 3.1, 3.3, can also be responsible for making the gateway unreliable. Consequences of an unreliable gateway on the LEMS include mainly inefficient management of the energy, financial losses, and data loss.

As the gateway plays such an important role in the energy management system, we need to employ measures that will help us detect as quickly as possible issues associated with it. An inexpensive and promising way to identify such problems is by using the side channel monitoring technique (SCM) [24]. SCM uses existing nodes as observers to monitor the gateway's packet transmission behavior. If any abnormalities are noticed, they will be reported back to LEMS. Although this technique is efficient, it can be easily detected by attackers and the reports could also be manipulated or intercepted. Therefore, as the detection of issues regarding the gateway is not guaranteed, multipath routing could also be employed to increase the probability of the data being delivered from the Gateway to LEMS and to the IoT [25]. Finally, in case that multiple unreliable gateways appear on the LEMS and the multipath routing also fails, to extend its functionality, the whole system could switch from using Wi-Fi to using the relatively reliable 3G network for data communication [25]. However, the cost of this solution is significantly high.

4 Conclusion

With the advancement of technology a gradual shift of energy management systems to the cloud has been seen, to overcome computational challenges faced by conventional energy management system. However, as we expose each component to the internet, to move to the cloud, the complexity and security of the system increases. In this paper we have given an overview of a cloud based energy management system by using a live example of a cloud based local energy management system (LEMS).

LEMS Vulnerabilities		
Risks	**Attacks**	**Target**
Data Leakage	Data Sniffing and MITM	Transmitted Data
Spoofing	Sybil Attack	System Blackout
Disruption of Service	DoS/DDoS	System Availability
Energy Bleeding	Barrage and Sleep Deprivation	System's energy resources
Hardware Issues	Faulty Gateways	Transmitted Data

Table 1

The aim of LEMS is to reduce the aggregated energy demand of a commercial building by using a set of electric vehicles and energy storage units available at building sites. Furthermore, we have addressed security concerns for the algorithm in the cloud as well as for the attached IoT devices. Each concern is explored by creating an attack scenario to identify vulnerabilities and best countermeasures for each attack is presented for that scenario.

In a cloud based energy management system, five major risks were identified and included: Data Leakage, Spoofing, Disruption of Service, Energy Bleeding, and Hardware issues, as per table 1. For each one of this risks, we described in detail the attacks associated with it and current defence mechanisms. We concluded that, although various measures to defend against these attacks have been proposed, none can fully guarantee the protection of the system. However, we hope this paper will act as a guideline to build a robust and lightweight security architecture to secure it.

References

1. K. Ashton. That internet of things thing. *RFiD Journal*, 22(7):97–114, 2009.
2. M. B. Barcena and C. Wueest. Insecurity in the internet of things. *Security Response, Symantec*, 2015.
3. S. Bera, S. Misra, and J. J. Rodrigues. Cloud computing applications for smart grid: A survey. *IEEE Transactions on Parallel and Distributed Systems*, 26(5):1477–1494, 2015.
4. T. Bhattasali, R. Chaki, and S. Sanyal. Sleep deprivation attack detection in wireless sensor network. *arXiv preprint arXiv:1203.0231*, 2012.
5. J. Diaz-Montes, M. AbdelBaky, M. Zou, and M. Parashar. Cometcloud: Enabling software-defined federations for end-to-end application workflows. *IEEE Internet Computing*, 19(1):69–73, 2015.
6. J. Diaz-Montes, Y. Xie, I. Rodero, J. Zola, B. Ganapathysubramanian, and M. Parashar. Exploring the use of elastic resource federations for enabling large-scale scientific workflows. In *Proc. of Workshop on Many-Task Computing on Clouds, Grids, and Supercomputers (MTAGS)*, pages 1–10, 2013.
7. T. Dierks. The transport layer security (tls) protocol version 1.2. 2008.
8. M. Dlamini, M. Eloff, and J. Eloff. Internet of things: emerging and future scenarios from an information security perspective. Southern Africa Telecommunication Networks and Applications Conference, 2009.
9. R. Falk and S. Fries. Managed certificate whitelisting–a basis for internet of things security in industrial automation applications. *SECURWARE 2014*, page 178, 2014.
10. M. Farooq, M. Waseem, A. Khairi, and S. Mazhar. A critical analysis on the security concerns of internet of things (iot). *International Journal of Computer Applications*, 111(7), 2015.
11. T. Fossati and H. Tschofenig. Transport layer security (tls)/datagram transport layer security (dtls) profiles for the internet of things. *Transport*, 2016.
12. A. Frier, P. Karlton, and P. Kocher. The ssl 3.0 protocol. *Netscape Communications Corp*, 18:2780, 1996.

13. O. Garcia-Morchon, S. Kumar, R. Struik, S. Keoh, and R. Hummen. Security considerations in the ip-based internet of things. 2013.
14. T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle. Security challenges in the ip-based internet of things. *Wireless Personal Communications*, 61(3):527–542, 2011.
15. R. Hummen, H. Wirtz, J. H. Ziegeldorf, J. Hiller, and K. Wehrle. Tailoring end-to-end ip security protocols to the internet of things. In *Network Protocols (ICNP), 2013 21st IEEE International Conference on*, pages 1–10. IEEE, 2013.
16. A. Jha and M. Sunil. Security considerations for internet of things. *L&T Technology Services*, 2014.
17. L. Ji, W. Lifang, and Y. Li. Cloud service based intelligent power monitoring and early-warning system. In *Innovative Smart Grid Technologies-Asia (ISGT Asia), 2012 IEEE*, pages 1–4. IEEE, 2012.
18. Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu. Security of the internet of things: perspectives and challenges. *Wireless Networks*, 20(8):2481–2501, 2014.
19. P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits. Denial-of-service detection in 6lowpan based internet of things. In *Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on*, pages 600–607. IEEE, 2013.
20. H. Kim, Y.-J. Kim, K. Yang, and M. Thottan. Cloud-based demand response for smart grid: Architecture and distributed algorithms. In *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, pages 398–403. IEEE, 2011.
21. J. Krishnaswami. *Denial-of-service attacks on battery-powered mobile computers*. PhD thesis, Virginia Polytechnic Institute and State University, 2004.
22. J. Laustsen. Energy efficiency requirements in building codes, energy efficiency policies for new buildings. *International Energy Agency (IEA)*, pages 477–488, 2008.
23. X. Li and J.-C. Lo. Pricing and peak aware scheduling algorithm for cloud computing. In *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES*, pages 1–7. IEEE, 2012.
24. X. Li, R. Lu, X. Liang, and X. Shen. Side channel monitoring: Packet drop attack detection in wireless ad hoc networks. In *Communications (ICC), 2011 IEEE International Conference on*, pages 1–5. IEEE, 2011.
25. X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin. Smart community: an internet of things application. *IEEE Communications Magazine*, 49(11), 2011.
26. Z. Li and M. Parashar. A computational infrastructure for grid-based asynchronous parallel applications. In *Proceedings of the 16th international symposium on High performance distributed computing*, pages 229–230. ACM, 2007.
27. X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato. Sage: a strong privacy-preserving scheme against global eavesdropping for ehealth systems. *IEEE Journal on Selected Areas in Communications*, 27(4):365–378, 2009.
28. K. Maheshwari, M. Lim, L. Wang, K. Birman, and R. van Renesse. Toward a reliable, secure and fault tolerant smart grid state estimation in the cloud. In *Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES*, pages 1–6. IEEE, 2013.
29. C. P. Mayer. Security and privacy challenges in the internet of things. *Electronic Communications of the EASST*, 17, 2009.
30. J. D. Montes, M. Zou, R. Singh, S. Tao, and M. Parashar. Data-driven workflows in multi-cloud marketplaces. In *2014 IEEE 7th International Conference on Cloud Computing*, pages 168–175. IEEE, 2014.
31. V. Moonsamy and L. Batten. Mitigating man-in-the-middle attacks on smartphones-a discussion of ssl pinning and dnssec. In *Proceedings of the 12th Australian Information Security Management Conference*, pages 5–13. Edith Cowan University, 2014.
32. U. of Waikato. Weka 3 - data mining with open source machine learning software in java. `http://www.cs.waikato.ac.nz/ml/weka/`, 2017. (Accessed on 01/13/2017).
33. OWASP. Man-in-the-middle attack. `https://www.owasp.org/index.php/Man-in-the-middle_attack/`, 2016. Accessed: 18/04/2016.
34. L. Pérez-Lombard, J. Ortiz, and C. Pout. A review on buildings energy consumption information. *Energy and buildings*, 40(3):394–398, 2008.
35. A. Perrig, J. Stankovic, and D. Wagner. Security in wireless sensor networks. *Communications of the ACM*, 47(6):53–57, 2004.
36. M. Pirretti, S. Zhu, N. Vijaykrishnan, P. McDaniel, M. Kandemir, and R. Brooks. The sleep deprivation attack in sensor networks: Analysis and methods of defense. *International Journal of Distributed Sensor Networks*, 2(3):267–287, 2006.
37. S. Poslad, M. Hamdi, and H. Abie. Adaptive security and privacy management for the internet of things (aspi 2013). In *Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication*, pages 373–378. ACM, 2013.
38. U. N. E. Programme. Why buildings. `http://www.unep.org/sbci/AboutSBCI/Background.asp`, 2016. (Accessed on 01/11/2017).
39. T. Rajeev and S. Ashok. A cloud computing approach for power management of microgrids. In *Innovative Smart Grid Technologies-India (ISGT India), 2011 IEEE PES*, pages 49–52. IEEE, 2011.
40. D. R. Raymond and S. F. Midkiff. Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Computing*, 7(1), 2008.

41. M. Saxena. Security in wireless sensor networks-a layer based classification. *Department of Computer Science, Purdue University*, 2007.
42. Y. Simmhan, S. Aman, A. Kumbhare, R. Liu, S. Stevens, Q. Zhou, and V. Prasanna. Cloud-based software platform for big data analytics in smart grids. *Computing in Science & Engineering*, 15(4):38–47, 2013.
43. Y. Simmhan, A. G. Kumbhare, B. Cao, and V. Prasanna. An analysis of security and privacy issues in smart grid software architectures on clouds. In *Cloud Computing (CLOUD), 2011 IEEE International Conference on*, pages 582–589. IEEE, 2011.
44. F. Stajano and R. Anderson. The resurrecting duckling: security issues for ubiquitous computing. *Computer*, 35(4):supl22–supl26, 2002.
45. H. Suo, J. Wan, C. Zou, and J. Liu. Security in the internet of things: a review. In *Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on*, volume 3, pages 648–651. IEEE, 2012.
46. L. Tang, J. Li, and R. Wu. Synergistic model of power system cloud computing based on mobile-agent. In *Network Infrastructure and Digital Content (IC-NIDC), 2012 3rd IEEE International Conference on*, pages 222–226. IEEE, 2012.
47. B. A. Ugale, P. Soni, T. Pema, and A. Patil. Role of cloud computing for smart grid of india and its cyber security. In *Engineering (NUiCONE), 2011 Nirma University International Conference on*, pages 1–5. IEEE, 2011.
48. Y. Wang, G. Attebury, and B. Ramamurthy. A survey of security issues in wireless sensor networks. 2006.
49. Y. Wang, S. Deng, W.-M. Lin, T. Zhang, and Y. Yu. Research of electric power information security protection on cloud security. In *Power System Technology (POWERCON), 2010 International Conference on*, pages 1–6. IEEE, 2010.
50. M. Wen, R. Lu, K. Zhang, J. Lei, X. Liang, and X. Shen. Parq: A privacy-preserving range query scheme over encrypted metering data for smart grid. *IEEE Transactions on Emerging Topics in Computing*, 1(1):178–191, 2013.
51. T. Weng and Y. Agarwal. From buildings to smart buildingssensing and actuation to improve energy efficiency. *IEEE Design & Test*, 29(4):36–44, 2012.
52. D. Wijayasekara, O. Linda, M. Manic, and C. Rieger. Mining building energy management system data using fuzzy anomaly detection and linguistic descriptions. *IEEE Transactions on Industrial Informatics*, 10(3):1829–1840, 2014.
53. C.-T. Yang, W.-S. Chen, K.-L. Huang, J.-C. Liu, W.-H. Hsu, and C.-H. Hsu. Implementation of smart power management and service system on cloud computing. In *Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2012 9th International Conference on*, pages 924–929. IEEE, 2012.
54. A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. Internet of things for smart cities. *IEEE Internet of Things journal*, 1(1):22–32, 2014.
55. K. Zhang, X. Liang, R. Lu, and X. Shen. Sybil attacks and their defenses in the internet of things. *IEEE Internet of Things Journal*, 1(5):372–383, 2014.
56. Y. Zhang. Technology framework of the internet of things and its application. In *Electrical and Control Engineering (ICECE), 2011 International Conference on*, pages 4109–4112. IEEE, 2011.
57. K. Zhao and L. Ge. A survey on the internet of things security. In *Computational Intelligence and Security (CIS), 2013 9th International Conference on*, pages 663–667. IEEE, 2013.
58. T. Zia and A. Zomaya. Security issues in wireless sensor networks. In *Systems and Networks Communications, 2006. ICSNC'06. International Conference on*, pages 40–40. IEEE, 2006.