Key Management Systems for Smart Grid Advanced Metering Infrastructure: A Survey

Amrita Ghosal and Mauro Conti, Senior Member, IEEE

Abstract—Smart grids are evolving as the next generation power systems that transform the traditional ways of functioning of present electrical grids. Advanced metering infrastructure (AMI) is one of the key components in smart grids. An AMI comprises of systems and networks, that are responsible for collecting and analyzing data received from smart meters. In addition, AMI also manages the different applications related with power and services based on the data collected from smart meters. Thus, AMI plays a significant role in the smooth functioning of smart grids. Malicious adversaries have immense opportunities for attacking the AMI, as it is made up of systems that are highly vulnerable to such attacks. Providing security to AMI is necessary as adversaries can cause potential infrastructural damage and privacy threats in smart grid. One of the most effective and challenging topic’s identified, is the key management system (KMS), for sustaining the security concerns in AMI. Therefore, KMS seeks to be a promising research area for future development of AMI. To the best of our knowledge, this survey is the first to highlight the significance of KMS for the security point of view for AMI in smart grids. We believe that we have taken here the needed initiatives that will help understand the importance of key management in AMI security, and strengthen future research works carried out in this area. This survey highlights the key security issues of AMIs and focuses on how key management techniques can be utilized for safeguarding AMI. At first, we discuss the main features of AMIs, the deployment scenario of smart grids and identify the relationship between smart grid and AMI. Then, we explore the main features of AMI, and also introduce the security issues and challenges. We also provide a discussion on the role of key management in AMI, and point out the differences between traditional electrical systems and smart grids. We then classify and provide a review of the existing works in literature that deal with secure KMS in AMI. Finally, we summarize the possible future open research issues and challenges of KMS in AMI.

Index Terms—Advanced metering infrastructure, key management system, smart grid, smart meters.

I. INTRODUCTION

SMART Grids are revolutionizing the conventional services provided by present electrical grid systems through the use of information technology [1], [2]. Also, maximum utilization of information technology is done in smart grids for achieving system efficiency and reliability [3]. Smart grids consist of power generation and transmission utilities in addition to, appliances, meters, sensing devices, information gateways that operate in near real-time [4]. The smart meters perform the tasks of collection of energy consumption, sending price information report to customers and informing about energy loss/restoration. The smart grids deploy sensing devices that are responsible for observing the performance of the system along with detection of any operational glitches. Upon detection of any failure, control messages are transmitted from the sensing devices to the control center. As the smart meters are located far from the utility, therefore, the data of the smart meters are routed to the utility via intermediate devices. The function of the gateways (also called concentrators), is to collect the data of the smart meter and send it to the utility using Wide Area Network (WAN) connection. The gateways also propagate control information to the smart meters.

For realizing the two-way communication [5]–[7] the architecture of smart grid is developed in such a manner that, the sensing devices, gateways, the smart meters and the control centers are present in the route between the customers and the power suppliers. The designing of smart grid encompasses many factors, but in general, synchronization between the fields of communication, control and optimization is very much required. From the ideal viewpoint, the design of smart grid must provide for adaptability, reliability and prediction issues. The designing process should also take into consideration the challenges involved, such as variations in demand and load handling, security, optimization of asset and cost, performance and power of self-healing [8]. In general, a smart grid communication system is composed of a combination of one or more regional control centers. Multiple power plants and substations are supervised by each center [5]. Figure 1 shows the structure of a smart grid communication system that does data collection and control of electricity delivery. The smart grid consists of components such as, regional control center, substation, smart metering system and power plants [9]. The regional control center performs the task of supporting the metering system, data management, operations of the power market and data acquisition control. The components of a substation are Remote Terminal Units (RTUs) [10], [11] circuit breaker, log servers, human machine interfaces, communication devices and gateways (data concentrators). Intelligent electronic devices that are basically field devices, consist of transducers, phase measuring units, tap changers and protection relays [5].

Manuscript received June 4, 2018; revised November 28, 2018 and January 31, 2019; accepted March 23, 2019. Date of publication March 28, 2019; date of current version August 20, 2019. (Corresponding author: Amrita Ghosal.)

The authors are with the Department of Mathematics, University of Padua, 35121 Padova, Italy (e-mail: amrita.ghosal@math.unipd.it; conti@math.unipd.it).

Digital Object Identifier 10.1109/COMST.2019.2907650
A. Global Outlook

Since the past few years, several countries worldwide, brought in mandatory legislations for adoption of smart metering networks for enabling clean energy initiatives [12]. In the EU, the EU member states have committed for roll-out of nearly 200 million smart meters for electricity by 2020 as a part of the third energy package resolution. Research shows that by 2020 almost 72% of the European consumers will have smart meters for electricity [13], [14]. The EU has already launched 400 smart grid projects, out of which about 90 projects deal with smart metering roll-outs [15]. It is estimated that over 237 million smart electricity meters will be installed across Europe by 2020. Likewise, in the U.S., the Smart Grid investment grant program under the American Recovery and Reinvestment Act of 2009 facilitates deployment of large scale deployment of smart metering infrastructures [16]. An instance shows that electric utilities in the U.S., in 2016 had about 70 million smart metering infrastructure installations, of which 88% were household consumers. The United States is another large market of smart electricity meters.

In Canada, more than 6 million smart meters were installed in 2014 and the number is expected to increase by 2016, where two thirds of the households in Canada will have smart meters [17]. Many places in Canada, such as, Ontario, British Columbia, Saskatchewan, and Quebec have already implemented or intend to implement a SM roll-out [18]. Till date, the most successful deployment identified is the Ontario Smart Metering initiative, having nearly 4.5 million installations of smart meters. For the Asia-Pacific region, China is by far the country having the largest number of installed smart meters. The study in [19] reveals that the growth of installed base of smart meters will increase to 377 million units by 2020 in China. In China, the 12th five year plan Energy Development, and the Strategic Action Plan on Energy Development (2014-2020) [20] carries out the smart grid deployment program. It is expected that the installation figures of smart meters in China will double by 2020. In Japan, the government has set a target for about 80% of the nationwide electricity consumption to be monitored using smart meters. The rough 80 million residential customers in Japan are expected to have smart meters installed in their homes by 2024. TEPCO, one of the main power utilities in Japan announced the roll-out program from 7 million to 27 million smart meters, more specifically, for household consumers. Installations started in the year 2014 and are expected to be completed by 2021. The Australian government mandated the roll-out of the smart metering program in 2009 which ended in 2013 with 2.8 million installation of smart meters having radio frequency mesh technology and WiMAX. Pilot projects are taking place in India for setting the stage for widespread deployment of smart meter, expecting to ultimately be more than 150 million new devices. Smart meter installation started in New Delhi in 2008 and continued to deploy 500,000 smart meters till 2011. Analysis of industry reports reveal that India will install 130 million smart meters having both Power Line Communication (PLC) and wireless technologies by 2021 [21].

B. Smart Grid and Advanced Metering Infrastructure

Advanced Metering Infrastructure (AMI) [22], that also goes by the name “smart metering” [23] is a critical component, that necessitates the realization of the vision of “Smart Grid”. In general, AMI consists of the smart meters [24]–[26] concentrators and the Meter Data Management System (MDMS) [27]. The smart meters consists of the communication board and the meter board that are connected using a serial port. The communication board handles the task of communicating with external nodes such as collectors or home appliances for execution of the required computations. Important information in the form of keys and passwords required for securing communication, are stored in the set of tables present in the meter board. The power consumption measurements are also performed by the meter board. The communication board uses an interrupt based mechanism for obtaining data or other needed information from the meter board. The data is then finally sent to the utility by the communication board. The MDMS is an essential component in AMI and basically serves as a database for long term data storage and management of events and data usage.

AMI also facilitates two-way communication [8], [28] between meter and distribution system operator. The two-way communication facilitates operations of many services for the distribution system operator that were nearly impossible to implement without smart metering. For example, power outage is detected faster by system operator and without interaction with the customer. Another service provided by smart metering is reporting the quality of the power delivered. Smart metering also enables detailed monitoring of power flows within the distribution system that was previously available.
only at the substation level. Monitoring of power flows is important as it enables energy suppliers to react quickly on variations in consumption levels. The power flow monitoring information is also useful for real-time pricing, that is handled by one technology in smart grid known as Demand Side Management (DSM) [29]. Recent advancements on smart metering technologies in smart grid have made several utilities and states to induce different time-based pricing initiatives. For instance, the Illinois power company in the United States, many critical peak pricing projects in California and New Jersey used a day ahead time pricing tariff. Recent works on smart metering have revealed that exposing end use consumers to hourly real-time prices is the most efficient technique to make the consumers consume electricity wisely and efficiently [30]. Additionally, in other countries such as, Denmark, Italy, Sweden, France, companies are replacing conventional meters with meters capable of giving real-time pricing. The utility NRGI in Denmark installed about 200,000 smart meters with a Home Area Network (HAN) interface for enabling energy awareness. In Italy, the distribution company of Enel group through their Telegstore project replaced old mechanical meters with an automated system that can protect the delivery system from frauds and energy theft, reducing the costs for interventions and improving the accuracy and efficiency of the billing process. Therefore, real-time pricing was improved by implementing the Telegstore project. The Swedish company Sundsvall Elnat AB is trying to install a smart meter consisting of a simple display at the customers premises. In France, the 300,000 smart meters installed by Enedis Operator will communicate to in-home devices using ZigBee interface. All these findings showcase that, gradually the concept of real-time pricing is coming into effect, mainly for the beneficial effects on the end consumers. Real-time pricing may be possible if energy costs is made variable, depending on the information of the present current power flow. This particular feature of the demand side management, provides the energy supplier to influence direct and immediate energy consumption [31].

The use of wireless communication in AMI leads to security issues in such systems. There are several security issues with regard to AMI that needs attention, ranging from the consumer level to the generation as well as the producer level. The adversary can launch an attack by sending false signals to meters that may lead to power outage in a particular area as well as disturb the demand generation model. The adversary can also make use of the study of the utilization pattern of the consumers for devising new forms of attacks.

Similar to other existing systems, AMI too needs to adhere with the requirements of the security primitives of confidentiality, integrity, availability [32] and non-repudiation.

- **Confidentiality** is preserved in AMI by ensuring that the energy consumption pattern of consumers are not revealed to unauthorized entities.
- **Integrity** is maintained in the system through detection of illegal data alteration.
- **Availability** requires the accessibility of data by an authorized user on demand. If the required data is not found at the time of need, the system violates the availability aspect of the security requirement of the system. Any natural or intentional incidents (such as hacking) must not hamper the system from operating correctly. For example, if the hacker wants to jam the network, the system must comply with the availability aspect.
- **Accountability** (non-repudiation) means an action that cannot be denied, i.e., the entities cannot deny the receiving or transmission of data. In the AMI network, accountability can be ensured through a timely response to the command and control, etc.

To meet the security requirements stated above, cryptographic countermeasures must be deployed. In AMI, cryptographic mechanisms are provided for by an efficient key management [33], [34]. If key management is not satisfactory, it may cause exposure of keys to attackers, and hamper the secure communications in AMI [35]. Therefore, key management is a critical process and can be used as a defensive mechanism against threats and vulnerabilities [36]. Generally, AMI involves the security requirements for confidentiality, integrity, and availability [37], [38]. Prior to AMI deployment, the primary security requirements such as protecting the privacy of customers by confidentiality, ensuring message authentication for meter readings and Demand Response (DR) [39], must be provided. Encryption and authentication protocols, rely heavily on the security of cryptography keys for ensuring confidentiality and integrity.

C. Contributions and Organization

In AMI systems, key management for a large number of devices is very much essential for security preservation of cryptographic keys. Recently, several studies were conducted related to the Key Management System (KMS) [35], [40], [41] of AMI, a vivid description of the same is provided in Section III. Existing surveys on smart grids discussed topics on cyber security [3], protection [6], smart metering [29], communication [32], architectures [42], and applications [43]. Different from [3], [6], [29], [32], [42], [43], this survey work deals with key management systems for smart grid in AMI, a very critical area where very less attention has been paid to. Unlike the existing survey works, this survey showcases the importance of AMI in smart grids and also focuses on the key management system that plays a defensive role in AMI against threats. To the best of our knowledge, this survey is the first to demonstrate the importance of key management system related to security concerns of AMI in smart grid. The novelty of this survey is in the classification of the existing works and outlining of future research in key management system of AMI. The main contributions of this survey are:

- We discuss the significance of AMI in smart grids as well and provide a classification for the current state-of-the-art works in key management systems of AMI.
- We provide a comprehensive discussion on the system structure of AMI, followed by the issues and challenges faced by AMI.
- We classify the existing works in literature, based on their commonality in approaches.
- We present a comparative study for the existing works in key management system schemes in AMI, considering
communication, computation and storage overheads as performance metrics. The metrics chosen for the comparative analysis reflect the efficiency of the corresponding scheme.

- We present promising directions for future research in smart grids, particularly in the area of advanced metering infrastructure where further research is required.

The rest of this paper is organized as follows. In Section II, description of AMI system features, followed by security challenges and the role of key management system in AMI are carried out. The classified approaches for existing key management systems in AMI are discussed in Section III. In Section IV, we present a comparative study for the current state-of-the-art key management schemes proposed for smart grid AMI. Finally, we identify the future directions and provide conclusion in Sections V and VI, respectively.

II. BACKGROUND

This section provides an insight into the Advanced Metering Infrastructure including the system features (Section II-A) together with the various security challenges (Section II-B) involved in such a system. We discuss the role of key management systems in AMI in Section II-C.

A. AMI System Features

1) Introduction: The Advanced Metering Infrastructure is referred to as the system responsible for collecting, measuring and analyzing the use of energy of networks that are connected to the smart meters. The components that make up an AMI are software, hardware, customer associated systems, communication networks and a MDMS [44]–[46]. Similar to other systems, the smart grid AMI also faces both internal and external security threats. The utility services of AMI provided to customers should ensure that the adapted security technologies are not vulnerable to adversarial activities. Deploying AMI in smart grid should guarantee confidentiality of user privacy along with authentication for meter readings and control messages.

A traditional AMI communication architecture shown in Fig. 2, has a centralized MDMS surrounded by the main operation and management services. The MDMS comprises of analytical tools that facilitates the interaction between operation and management systems including Outage Management System (OMS), Geographic Information System (GIS), Consumer Information System (CIS) and Distribution Management System (DMS).

2) AMI System Structure: An AMI is perceived as an infrastructure that integrates several technologies for achieving certain specific objectives. Figure 3 describes the components of the AMI system structure that are briefly discussed below:

Smart Meters (SMs): Electrical meters that perform the operations of providing two-way communication [47], collection of automated meter data, outage management and dynamic pricing.

Distributed Energy Resources (DERs): Electricity generation systems that are small scale and renewable and are used for storing energy and in homes [48].

Gateways (GWs): Execute the task of accomplishing conversion of protocol and communication among two heterogeneous networks. Examples of gateways are home area network and wide area network.

Wide Area Communication Infrastructure: Performs the task of bidirectional communication between the costumer domain and the utility system. Such infrastructures use architectures and medias such as power line communication system and cellular networks [49].

Meter Data Management System (MDMS): This is a database system used for storage, management and analysis of metering data for providing better customer services [50].

Demand Response (DR) Program: It is basically an agreement between the utility and its customers. The agreement provides for ensuring the customer of reduction in tariffs or...
discounts in the electricity bill, on the condition that he agrees to reduce his electricity consumption in response to signals received by the grid. The basic concept of the demand response program is that if every customer conserves a little, there will be enough power for everyone [29]. The different demand response programs that are currently existing have their own policies in terms of rewards, penalties and consumer notification policies. The benefits of all these demand programs are same irrespective of their particular characteristics.

From communication perspective, the AMI comprises of the following networks.

**Home Area Network (HAN):** This type of network connects smart meters and smart devices within home premises [42], [51]. It also provides low cost monitoring and control of the electronic devices to reduce energy consumption. Both low range wired and wireless technologies are used for building such networks, though wireless technologies such as 802.11 wireless networking protocol, ZigBee and HomePlug [52] are more dominant. The smart meters are made up of many sensors and data sources. Lightweight security mechanisms are needed for the sensors used in the smart meters as they are generally resource constrained [53].

**Wide Area Network (WAN):** This network performs the task of connecting an AMI end in the local utility network and a data concentrator [54], [55]. Data is collected from a group of SMs by the data concentrator. The data concentrator is responsible for sending the collected data to the headend. The information exchanges between external systems, such as MDMS and AMI network is performed by the AMI headend.

**Neighborhood Area Network (NAN):** It is mainly formed by combining a number of HANs. In this network, several necessary information such as, security alarm and data of power consumption are transmitted for achieving energy management [43], [54].

**Smart Meter Gateway (SMGW):** It is the central communication component of smart grid infrastructure. The gateway forms a connection between a WAN and a network of devices of one or more smart meters. The communication between the consumer and is consuming and generating devices are maintained and secured from physical attacks by the SMGW [56]. The security module of SMGW performs the task of providing authentication and aggregation of messages sent by the meters to the control center [57].

3) **Appliance Load Monitoring:** Recently, the issues related to the energy conservation and efficiency in smart grid have gained a significant importance from both consumer and energy supplier point of view. To address these issues, the researchers developed Appliance Load Monitoring (ALM) techniques [58], [59]. The main objective of ALM is to monitor and estimate the energy demand of each appliance in smart home. There are two categories of ALM, namely, Intrusive Load Monitoring (ILM) and Non-Intrusive Load Monitoring (NILM) [58]. In ILM, one or more than one sensor per appliance is used to perform ALM. On the contrary, in NILM, a centralized point is used to perform ALM in each appliance per home or building. The main advantage of ILM over NILM is that the more accurate load monitoring capability of ILM. However, due the high installation complexity and cost of ILM, NILM techniques are more popular than ILM for large scale deployments. Considering the advantage of NILM for large scale deployments, number of works [60]–[62] were done to improve the performance of NILM based approaches in a realistic environment. In one such work, researchers developed a smart electricity meter [63], called Powerley Energy Bridge (PEB), to measure electricity consumption in household appliances. The specialty of PEB is that it sends the latest electricity consumption measurements to a server in real time using Wi-Fi interface. PEB is also efficient in appliance health monitoring [64].

B. **AMI Security Challenges**

With the rapid growth in the development of smart grids especially in the context of smart cities, have led to further advancement in technologies such as AMI used in such systems. Security challenges in AMI [65] can in general result from three different aspects: privacy preservation of end users, system resilience against cyber attacks and power theft. The technical challenges that need to be addressed by the smart grid, is discussed in this section.

1) **Privacy Preservation of End Users:** The security issues related with smart grid and AMI continue to scale up considerably with increase in smart meters usages, both from internal as well as external part of the system. The consumers’ life style can be exposed from the information obtained from the consumers’ electricity energy consumption, resulting in a critical situation. Examples of leakage of critical information can be in the form of, alarm and security systems used, number of people living in a house, time of occupancy, appliance types, security and medical emergencies. Many studies have shown how vital information is obtainable by use of consumer profiling [66], [67]. Some work, such as [68] introduced techniques for improving the privacy protection of consumers data. The method used in [68] mainly reshapes the overall pattern of data such that it is impossible to differentiate between load patterns and signatures.

For expansion of AMI, consumers satisfaction is very much important. If poor service or power quality is experienced by the consumers, because of external factors such as, data alteration by unauthorized parties or hackers, then, they may provide hindrance toward the implementation of AMI. At the consumer side, the price signal and commands that are available, are also possible areas where physical and attacks may occur with the intention of destructing infrastructure or power theft. Also, long distance transmission and storage of data for retransmission or analysis, makes the data susceptible in terms of data theft or manipulation [8]. Considering all these factors, the government is working meticulously to guarantee information privacy of customers.

2) **System Resilience Against Cyber Attacks:** Cyber security is gaining importance in smart grid due to rising chances of cyber attacks and incidents in such power grids. Cyber security needs to address the deliberate attacks arising from dissatisfied employees, industrial spying, and terrorists. From the vulnerability view point, the attacker has the opportunity of entering into a smart grid network, and devise mechanisms to
destabilize the grid in different ways that are highly unpredictable. A smart meter is expected to retain its own digital credential and thereby guaranteed to obtain secure connections with the smart meter network. Even if a particular smart meter is compromised, the adversary should not be able to obtain critical information of other meters or gain access into the AMI of the smart grid.

The cyber security threats existing in the perspective of the general requirements for AMI security are summarized below:

- **Confidentiality:** Confidentiality as from the perspective of AMI is perceived protecting the privacy of consumer’s information and consumption pattern. Therefore, the system must provide for keeping the consumption information confidential. Also, the physical tampering of smart meter to illegally access the stored data as well as using other means of unauthorized access to the data by other mechanisms should be prevented [69]. At AMI head end, confidentiality of customer information should be maintained by allowing only authorized access to specific data sets.

- **Integrity:** Integrity with respect to AMI is applicable for data transmission from meter to the utility and control commands from utility to the meter. Integrity refers to the mechanisms involved for preventing alterations in the data received from meter, and in the commands sent to the meter [70]. The hackers possess a threat to the system integrity as they can launch attacks by pretending to be authorized entities. Smart meters are robust against cyber or physical attacks, compared to electromechanical meters. Smart meters must have the capability of ignoring the control commands raised due to cyber attacks and preserve the system integrity.

- **Availability:** The availability issue in AMI changes, depending on the type of information communicated in the system. The non-critical data can be collected keeping the time intervals longer, and instead of using actual data, estimated ones are used. In some scenarios, necessitates the collection of actual values in minimum time. The prime factor for data unavailability in AMI is failure of the component. The causes of component failure may be from problems arising due to software or due to meter tampering resulting out of human intervention. Another reason for unavailability in AMI can be communication failure. The reasons for communication failure include, network traffic, path degeneration, interference, bandwidth loss, etc.

- **Accountability:** It refers to the fact that data receivers will not deny receiving of data and vice versa. Thus, entities not receiving any data, cannot claim that they have done so. In AMI, accountability is significantly important from the view point of finance and control signal responses. The primary concern for accountability requirement is due to the components in AMI being manufactured by different vendors and owned by different entities. Synchronizing the time and precise time stamping of information are also necessary in the AMI network for ensuring accountability. The most common method of accountability maintenance is through audit logs. For accountability with respect to smart meters, all metered values, modifications in tariffs should be made accountable as they are the form of basis for billing.

3) **Power Theft Prevention:** Occurrence of electrical losses can be in any of the stages of generation, transmission, distribution, and utilization. Losses that take place during generation are technically more easily justifiable, than those that occur during transmission and distribution. Losses can also be categorized as technical loss and non-technical loss. Power dissipation in electrical lines and components lead to technical loss. On the other hand, detection and prevention of non-technical loss during transmission and distribution of electricity is difficult, thereby, leading to a major utility problem.

The use of electro-mechanical meters in traditional systems have minimum security features and are prone to manipulation. Electro-mechanical meter thefts are detected using the methods of direct connection to distribution lines and grounding the neutral wire [71]. The use of smart meters in advanced grids resulted in elimination or reduction in the above mentioned issues of electro-mechanical meters.

Certain techniques for power theft are not associated with the direct intervention with the meter. One example of such technique is tampering of the current transformer. Current transformers perform the matching operation of grid current rating with the meter rating for meters of large loads. Though the secondary side wires of current transformers are generally insulated, but still there is a possibility of harming the insulation and wire tapping. The tapping of the wires lead to erroneous meter readings. Another indirect method of power theft, is by exchanging the position of damaged wires, resulting in phase shift and modifications in the meter reading.

Some techniques used in electro-mechanical meters for stealing, is also applicable in systems with smart meters and AMI too. One such technique is data tampering. The occurrence of data tampering can happen during data storage in the meter, data collection and during data transition across the network. Data tampering due to collection is applicable for both smart and conventional meters. Data interference during storage and transition is only applicable for smart meters. Compared to conventional electrical systems, the use of data loggers in AMI results in difficulty in tampering meters. The loggers record the power outages to the meter as well power flow inversion. Thus, attack techniques involving inversion or disconnection, also need to remove logged events in the meter. The smart meter stores data of various types, such as, time of use tariffs, event logs, executed or received commands and the firmware. Attackers that are able to access the smart meter data, get all the vital information from the stored data. Data manipulation in another way can take place during its transmission over the network. Adversaries may launch attacks by injecting false data or by communication interception while the data is in transit.

Apart from the security issues and challenges discussed above which are common for both wired and wireless networks in AMI [72], we also discuss below the issues and challenges that exist from the aspect of wireless networks in AMI of smart grids.
Radio Waves Reception Problem: The problem of radio waves reception is a major challenge in wireless communication. The radio waves reception problem occurs when the waves are not received at the expected place and time. In AMI, meter data recorded by the smart meter is collected by the gateway and finally sent to the respective power company. Any problem in the communication path between the smart meter and the gateway, hinders the receiving of the recorded data. It is not feasible to deploy large number of gateways along the communication path to evade the problem of non-reception of recorded data. Therefore, communication paths should be configured such that radio waves arrive at the gateway after being sent from the smart meter.

Transmission Delay: As the transmission speed of wireless communication is lower than that of fixed-line communication, transmission time gets longer. Besides, when various meters generate data randomly, their radio waves interfere and do not reach the receiver side. The problem of transmission delay needs to be minimized for time critical smart grids.

Hidden Node Problem: Similar to other wireless networks, the hidden node problem can also occur in AMI. The hidden node problem hinders communication and prevents timely transmission of data to relevant receivers.

Radio Waves Collision: The problem of radio waves collision prevents the collection of the transmitted data to be 100%. To allow power companies to collect data with certainty, it is necessary to devise mechanisms for avoidance of collision radio waves.

Attack Vulnerability: Communication over a wireless network is vulnerable to attacks. An attack example scenario can be of an adversary reverse engineering the network protocol and disturbing the communication. Also, based on the knowledge of the protocol as well as the network structure, the adversary may leverage injecting of modified traffic (e.g., modified power consumption data) into the network between the smart meter and the public utility system.

Disruption Threat: Disruption threat refers to interrupting the system from operating in the right way. For example, wireless transmission among appliance, smart meter, and HAN gateway can be interrupted by an adversary through jamming.

Distributed Operation: A centralized communication architecture in the smart grid may lead to bottleneck in the system, as a large volume of data is generated and processed in such systems. Transmitting the high amount of data can develop a congestion readily and thereby, a congestion control procedure is needed. Also, the sensor nodes deployed in different locations of the power grid, cause scalability issues and a decentralized aggregation technique is very much required for sensor measurements. So, the communication network should be distributed to bypass a failure at the single point.

High Bandwidth: With the rapid expansion of smart grids, new components are introduced into the network. Therefore, bandwidth requirement becomes an important factor. For example, even for a power distribution system of moderate size, the bandwidth requirement is of 100Mbps and above. Bandwidth requirement can be compensated using optical fibers or by using Ethernet passive optical network.

Interoperability: The communication network should be flexible such that it can communicate with different types of sensors and actuators seamlessly. Also, there should be a synergy between different communication technologies such as PLC, fiber optic communications, and wireless communications.

Scalability: The communication network should be scalable due to the presence of several sensors and actuators in the network. It should be capable of adding or removing devices without the use of manual reconfiguration.

C. Role of Key Management Systems in AMI

As mentioned in Section I, AMI is a new emerging technology for smart grid, and is defined as the system used for collection, measurement, storage, and analysis of usage of energy data [73]. It also facilitates in building a bridge between consumers and electric power utilities. For delivering the future needs, certain techniques used in smart grids, expose them to cyber security threats. Similar to other systems, the cyber security requirements of AMI must adhere to the needs of protecting confidentiality, integrity, and availability. Therefore, before AMI deployment, the major security requirements as stated above, need to be provided. Earlier findings by researchers have demonstrated that key management plays a vital role in providing security to networks and communication systems. For example, the works in [74], [75] show how key management helps to achieve secure group communication. Also, the authors in [76] cite the importance of key management in mobile adhoc networks. Therefore, using key management in AMI systems is very much significant for providing protection to the different entities associated with such a system. The key management system generally comprises of a key organizational framework, key generation, refreshment, distribution, and storage policies [77].

Smart grid comprises of heterogeneous communication networks. The communication networks include, time-critical (e.g., for protection purpose) and non-real time (e.g., for maintenance work) networks, small-scale (e.g., a substation system) and large-scale (e.g., the AMI system) networks, wireless and wired networks. Therefore, considering the practical scenario, it will not be wise step to design a single key management infrastructure for key generation and distribution, that caters to all networks in the smart grid. So, key management schemes in smart grids should be chosen judiciously, for fulfilling the network and security requirements for the different systems in smart grid.

The traditional key management framework considers the use of single symmetric key among all users [3]. Though the use of a single key is beneficial from the efficiency point of view, it is the least secured mechanism for providing secure communication. If an attacker gets the key by compromising a device, it can very easily inject false information in the entire network. In the existing metering system, the same symmetric key is shared between all meters. Also, existing key management schemes for traditional power system, use neither a full-fledged key management infrastructure, nor support efficient multicast and broadcast that are essential for smart
The users subscribed to a DR project are not fixed and therefore, it is required to update the group members periodically who receive the multicast messages. In multicast communication, key management consists of two parts, where, one part has similarity with the broadcast communication. For the first part, before each new session, the session key for multicast communication should be generated. The second part is involved with the regeneration of the group key and additional values that are refreshed using unicast communication.

III. KEY MANAGEMENT APPROACHES

According to [50], key management systems are an important part of AMI that facilitates secure key generation, distribution and rekeying. Different approaches were adapted for ensuring efficient key management. In the literature authors reported works that deal with the issue of key management system. All these works are conducted through different approaches based on different secure key generation and distribution mechanisms. In this survey we categorize the existing works, mainly into four categories, namely, key graph technique, encryption based technique, Physically Unclonable Function (PUF) based technique and hybrid technique. In Fig. 4, we provide a classification of the state-of-the-art works in the area of KMS in AMI of smart grids, which we have analyzed in the following sections.

A. Key Graph Technique

By far, key graph technique is the most commonly used key management mechanism due to the ease of implementation and efficient performance. The key graph technique can be classified into two categories, namely, multi-group key graph technique and tree key graph technique. The following subsections provide description of the works under the above mentioned classification.

1) Multi-Group Key Graph: This section illustrates the state-of-the-art works that adapted multi-group key graph technique for secure key management in AMI.

Authors in [83] secure unicast, broadcast and multicast communications through implementation of scalable multi-group key graph technique for key management in AMI. This work also safeguards the AMI security requirements. The multi-group key graph structure used here, supports the management of multiple demand response projects concurrently for every customer. Here, establishing the individual keys between the smart meters and MDMS is achieved by use of specific and secure exchange of cryptographic keys over a public channel. The individual keys that are refreshed periodically are used in two ways. In the first method, securing the unicast communication takes place between MDMS and SMs, while the second provides for secure multicast communications by generating the multi-group key graph. The MDMS is responsible for generating a group key that is also refreshed periodically for the DR project. The generation and transmission of group key takes place through secure channels for each SM.

The scalability issue is addressed using Logical Key Hierarchy (LKH), where a key tree is used for every DR
In LKH, each member keeps a copy of its leaf secret keys and all other keys of the nodes in the path originating from its leaf to the root. The authors demonstrate that using their proposed LKH, scalability is ensured for large smart grids with dynamic demand response projects. Also, to reduce storage and communication costs in key management, a multi-group key graph structure is proposed in this work. The proposed key graph technique allows multiple DR projects to share a new set of keys. The communication cost that occurs due to rekeying operations, is not significantly affected by the joining or leaving of a user of a DR project compared to that introduced by the use of separate LKH tree. In this work the multi-group key graph structure is modeled as a two level graph. The lower level, signifies the user set having the same first DR project subscription. In the lower level, the leaf node of the tree denotes a user’s individual key and the root of the tree is the group key of the DR project. The upper level graph represents the combinations of root keys for concurrent users subscribing to multiple DR projects. Authors claim that all these features ensure no redundancy in case of user subscription and payment for the same DR project multiple times.

In [84], the authors proposed a scalable multi-group key management for AMI for securing data communications in AMI. This work also supports key management in unicast, multicast and broadcast communications with the help of multi-group key graph technique. The simultaneous management of multiple DR projects for each customer, is supported by the multi-group key graph structure used. Also, the authors demonstrate that this new structure is very much applicable in large scale smart grids with dynamic DR projects memberships.

A particular method is used in this work for secure exchange of cryptographic keys over a public channel. The secure exchange of cryptographic keys is used between the MDMS and smart meters for individual key establishment. The individual keys are refreshed periodically and utilized in two ways. The first method secures unicast communication between MDMS and the SMs, while the second, provides the multi-group key graph for secure multicast communication. A group key must be generated by the MDMS and refreshed periodically for the DR project. The generation and transmission of the group key for every smart meter is done through secure channels.

The scalability issue is addressed by the use of the key graph technique known as One-way Function Tree (OFT), that is improvised over the LKH protocol. In OFT, the MDMS and all users individually compute the group key. Recursive computation is done for computing the keys of the interior nodes, from the keys of their children. For reducing storage and communication costs in key management, a multi-group key graph structure is proposed in this work. The key graph technique allows several DR projects to share a new set of keys. The two levels of lower and upper levels form the model for the multi-group key graph structure. The lower level comprises of OFT that represent a set of users with the same first DR project subscription. An user’s individual key is denoted by the leaf node, while the root of the tree represents the group key of the DR project. The users subscribed to multiple DR projects concurrently, are represented by the root key combinations in the upper level of the graph. Both backward and forward secrecy are supported by the proposed key management scheme. Security and performance analyses, and comparison results exhibit that the scheme induces low storage as well as low communication overheads.

Authors in [41] proposed four key management schemes that can simultaneously support security, scalability, efficiency and versatility. The first scheme named as Versatile and Scalable key management scheme for AMI (VerSAMI), is used in large-scale AMI system for ensuring secure unicast, multicast and broadcast communications. VerSAMI also supports the management of multiple DR programs. This is done to provide flexibility to customers in terms of subscription to multiple DR programs simultaneously. Also, the customers can subscribe/unsubscribe to any DR program at any time. Here, the rekeying operations are handled efficiently using the multi-group key graph technique, while meeting the constraints of smart meters with respect to memory and bandwidth capacities. An improved version of VerSAMI, called, VerSAMI+ is also proposed by the authors, that provides enhancement in communication overhead. The problems in VerSAMI as well as VerSAMI+ that occurred due to individual rekeying, and also to reduce the number of rekeying operations, another variant of VerSAMI, called Batch-VerSAMI was proposed.
by the authors. The alterations in memberships are handled in Batch-VerSAMI in batches, instead of handling individually. In addition, for simulating the AMI system behavior, the authors proposed a dynamic membership model. The efficiency of the proposed schemes are proved through security and performance analyses, as well as simulations, performed with existing schemes.

2) Tree Key Graph: This section describes the schemes that use the tree key graph as the structure for the key management system in AMI.

In [77], authors design a key management system for dealing with the security requirements in AMI. The key management framework of the AMI system is developed with the help of the key graph. This work designed key management processes of three types for supporting the hybrid transmission modes that also include key management for unicast, broadcast, and multicast modes. For minimizing the storage and computation constraints of SMs, simple cryptographic algorithms are chosen for key generation and refreshing policies. Designing of key refreshing policies are specific to the DR project, considering the inconsistencies in the number of members in a DR project. Mainly the key management framework based on the key graph concentrates on managing the keys of a large number of SMs. The security and performance analyses of the KMS demonstrate that the proposed scheme is a possible solution for AMI systems. The KMS is designed for collecting of the possible solutions, though the functions of AMI vary. In reality, flexibility is given to users for choosing part of the KMS for specific applications. The characteristics of transmitted messages in the communication channels is decided by the function requirements. The authors designed key management processes of three types for unicast, broadcast, and multicast communications, considering the types of messages and function requirements for the required mode of communication. Refreshing policies and key generation are designed specific to each process, considering computation and storage constraints of SMs.

In [85], the authors introduce Information Centric Networking (ICN) in AMI systems and also proposed a key management scheme for large number of smart meters for ensuring confidentiality, integrity and authentication. The scheme is designed with an objective to ensure security, control network congestion and support mobility. The energy data in AMI system needs to be kept secret as they can reflect the privacy of daily lives of people and habits. The use of ICN provides for data integrity as well as authenticity and confidentiality. It is different from the protection available in end-to-end communication as it depends on the protection of data itself. Here, secure message exchange for unicast, broadcast and multicast is ensured.

The ICN-AMI system structure shown in Fig. 5 develops the KMS frame structure by key graph similar to that of [86]. The user key, the group key and the root key is used for unicast, multicast and broadcast mode, respectively. The inherent feature of digital signature in ICN’s provides for authenticity and integrity. Here, the transmission modes of unicast, broadcast and multicast, are provided data confidentiality by payload encryption. For unicast transmission, four types of messages

![Fig. 5. ICN-AMI System Structure for Key Graph Technique.](image-url)
as brute force, replay as well as capable of minimizing the management overhead. Security and performance analyses are presented that demonstrate the desirable attributes of the presented scheme.

2) Two Level Encryption: This section describes the work based on two level encryption for key management system in AMI.

In [89], a key management scheme is proposed based on two level encryption method. The encryption is based on two partially trusted simple servers that implement this method without increasing packet overhead. One server is responsible for data encryption between the meter and control center and the other server manages the random sequence of data transmission. Authors further introduce one-class support vector machine algorithm for node-to-node authentication utilizing the location information and the data transmission history (node identity, packet size and frequency of transmission). This mechanism helps in securing data communication privacy without increasing the complexity of the conventional key management scheme. This work is an extension of one of the earlier work’s of the authors. The extended work uses Received Signal Strength (RSS) and One Class Support Vector Machine (OCSVM) techniques for node to node authentication. RSS is used for localization of meters using the received signal strength from neighbouring meters. OCSVM is used for detecting new and outlier data/packet, using current and previous data transmission history. Further, OCSVM based node authentication increases robustness in key management system without increasing any overhead and is easy to implement in devices with limited memory and computational ability. The introduction of two separate servers for key management and random sequenced packet transmission enhances robustness in security in untrustworthy communication medium and servers. Both qualitative and quantitative analyses reveal the scheme’s efficacy in providing improvements in the key management schemes of AMI.

C. PUF Based Technique

In contrast to key graph and hybrid techniques mentioned above, PUF based technique for secure key management in AMI has not been exploited much in the literature. This section mentions two such works in the area of PUF based KMS in AMI. One of them is based on broadcast group key management [90] while the other uses hash chain [91].

1) Broadcast Group Key Management: This section provides description for the work that utilizes the broadcast group key management technique in PUF base KMS.

In [90], the authors provide an end to end security for AMI networks. The model used here is based on weak PUFs [92]. PUFs are used as security primitive for providing robust hardware based authentication for smart meters and collectors. Fig. 7 shows a smart meter with a PUF System on Chip (SoC) that is used for this scheme. The initialization phase is utilized by the utility for generating a pair of challenges and three hash functions. The challenges are used for triggering the PUF responses, while, the hash functions are used for obtaining the hash codes and computing the symmetric key of the smart meter. The proposed approach provides efficient solution to manage keys and a robust authentication mechanism. The solution is developed using PUF devices that are cheap to manufacture and provide hardware based strong authentication mechanisms against spoofing attacks. The one way function of the hardware of the PUFs’ devices assist in generating and regenerating of the access level passwords for smart meters. Strong defense against key leakage is provided by the PUF based secret generation method as the key is not stored in memory. For supporting multicast communications, this work utilizes Broadcast Group Key Management (BGKM) scheme [93], [94]. The BGKM scheme is a special type of group key management scheme that allows for efficient communication of a group of nodes. The use of symmetric key cryptography in BGKM does not make it computationally intensive. The smart meter derives the group key from the unique secret designated to it. The efficiency and scalability of the BGKM scheme is supported by its capability of addressing any group of nodes with a single message.
2) **Hash Chain:** The work described in this section employs hash chain mechanism for PUF based KMS. Authors in [91] devised mechanisms for authenticated key exchange protocol and message broadcasting protocol utilizing the PUF technology in communication parties. The PUF is embedded in the head end system for key exchange protocol while in message broadcasting protocol, it is embedded in the smart meters. The PUFs are used for generating the commitments and random numbers that are required for running the protocols. The head-end system and the smart meter exchange a session key after mutual authentication. The key exchange protocol comprises of four phases, namely, initialization, registration, mutual authentication and key exchange. The authors, in this work exploited the idea of hash chain and a modified version of Schnorr protocol [95] for developing an authenticated broadcast messaging protocol for the AMI systems. The proposed protocol allows for automatic authentication of the headend by the smart meters. Thereby, the smart meters are ensured that the message received is broadcast by the head end. The message broadcasting protocol consists of three phases, initialization, registration and authentication. The security analysis of the proposed authenticated key exchange protocol proves its efficiency in terms of security requirements as well as the message broadcasting protocol is secured against corrupted smart meters.

**D. Hybrid Technique**

Hybrid techniques for KMS provide for both symmetric and asymmetric encryption for securing AMI in smart grids. Hybrid techniques are grouped under two categories, namely, ID based encryption and advanced encryption standard. This section provides description on potential works that deal with KMS using the hybrid techniques.

1) **ID Based Encryption:** The work in the following section describes how ID based encryption assist in hybrid key management in AMI.

In [50], the authors proposed a hybrid KMS for AMI through combination of public key and symmetric cryptosystems. Authentication and session key generation is achieved using elliptic curve cryptosystems. Also, the scheme makes use of a specially designed key hierarchy for efficient generation and updation of group keys. ID-based encryption is used by the KMS and the key graph technique is employed for efficient multicast key management. The primary benefit of using ID-based encryption lies in the fact that no public key certificate is required. The security issues of multicast key management and end-to-end key establishment are the main concerns of this work. The secure establishment of the session keys with each smart meter is performed by MDMS. The resulting session keys provide for scalable and efficient group key management for AMI. Security analysis and performance evaluation for this scheme reveal that it is secure and efficient for AMI in smart grid.

2) **Advance Encryption Standard:** The work in this section employs advance encryption standard for key management systems in AMI.

Authors in [4] proposed a hybrid encryption scheme as shown in Fig. 8, that exploits symmetric and asymmetric encryptions for securing smart metering network. The proposed method makes use of elliptic curve cryptography. The elliptic curve cryptography introduces a precomputation stage for minimizing the computation overhead through elimination of the time needed to perform the scalar-point multiplication. The hybrid mechanism developed in this work, combines the public key cryptography with the secret key encryption. A lightweight key management scheme is proposed here for reducing the overheads resulting due to key generation, distribution and renewal. Advance Encryption Standard (AES) is used for the data encapsulation cryptosystem, while, elliptic curve encryption is employed for the key encapsulation cryptosystem. The modules of the proposed hybrid encryption cryptosystem are symmetric encryption module, asymmetric encryption module and message integrity module. The encryption of AMI messages using AES-128 is performed by the symmetric encryption module. The asymmetric encryption module encrypts the arbitrary key used by the symmetric encryption module. The data encapsulation function is performed by the symmetric encryption module, while the key encapsulation system is taken care of by the asymmetric module. Message integrity module is used for generating the integrity code that enables detection of tampering of the secure message.

The messages transmitted using this proposed protocol has the packet format as follows: the payload field stores the information needed for sending to the destination. The synch and clock tolerance fields perform the function of protection against reply attack. The synch field stores the message timestamp corresponding to message creation time, whereas, clock tolerance indicates the message validity time. The synch field is compared with the current time on receiving a message. The message is considered replayed and is rejected, based on the time difference between the synch and the current...
time. The hybrid cryptosystem adds the encrypted arbitrary key to the message. The encrypted key is stored in the key field. Authentication ans message integrity is ensured by the Message Integrity Code (MIC). The MIC field helps in detection of a tampered message or a message originating from an unauthorized source. The results obtained demonstrate that the scheme performs well in terms of computation, storage and communication overheads. Also, the scheme is capable of defending eavesdropping and traffic analysis attacks with the help of message confidentiality.

IV. COMPARATIVE STUDY

The objective of this section is to provide a detailed analysis of the works that carried out efficient key management system of AMI in smart grids, in the perspective of both security and performance analyses. In Table I, we summarize the terminologies that are used throughout the remaining of this paper.

Table II highlights the security analysis of the various schemes. In this table, we provide an insight into how efficient the schemes are in comparison to each other by taking into consideration certain security parameters. The parameters considered are key generation, key sharing, key freshness, forward and backward security, confidentiality, authentication and integrity. On the other hand, performance analysis of the different schemes through computation cost, communication cost and storage cost are illustrated using three tables.

The processes of key generation, key sharing and key refreshment referred in Table II, are carried out through multiple steps that involve communication between different entities of AMI. It is important to provide optimized communication overhead for the processes of key generation, key sharing and key refreshment for time critical scenarios in AMI. Key refreshing is dependent on users joining or quitting the DR project. The group key is refreshed during the update, i.e., when an user joins or quits the DR project. The forward secrecy refers to the fact that new users participating in a DR project, should not be able to access previously used secret keys and messages. On the other hand, backward secrecy implies that users who leave a DR project are unable to access the future secret keys and messages. Forward secrecy, in terms of group key management, refers to the fact that evicted members will not have any knowledge of the new group key. With respect to group key management, backward secrecy means that new members cannot gather any knowledge about previous group keys. Preserving forward and backward secrecy should be guaranteed, considering the fact that users participating in DR projects are not consistent, and have the privilege of joining or leaving a DR project any time.

Table III and Table IV provide the comparative analysis of computation and communication costs, respectively of the various schemes. The computation cost of the key management protocols are divided into four parts: end to end key establishment, initializing group, adding a member and deleting a member for both MDMS and smart meter. Here, we provide brief descriptions of how computation costs are derived by each of the schemes compared in Table III. In [35], the computation cost is derived from two sources, namely, for establishing the end-to-end key protocol and the multicast key management protocol. The computation cost for the end-to-end key establishment protocol involves the calculation of two point multiplications, one bilinear pairing and two hashes. The calculation is done by both the smart meter and the MDMS. The computation cost for the multicast key management protocol comprises of three parts: group initialization, member addition and member deletion. The group initialization takes place only once in the proposed scheme. In [77], the computation cost is for every device on the user side and one device for the management side. For each device on the user side, the computation cost is formed due to symmetric cryptography algorithms, hash functions, and Hash Message Authentication Code (HMAC). The computation cost in MS is also due to symmetric cryptography algorithms, hash functions, and HMAC, same as that in the user side devices. Considering one example from Table III, the computation cost of the scheme SKM, for initializing a group, is higher than that of the scheme KMSSC. The results of Table III also reflect that, adding a member or evicting a member for the SKM scheme is much more efficient in comparison to KMSSC scheme. The scheme KMSSC does not mentions about the key establishment mechanism it uses, and so the cost involved for the end-to-end key establishment protocol is unavailable.

The benchmarks provided in Table IV, demonstrate the communication overhead of the different schemes. The comparative study is done using unicast and broadcast communication for both member addition as well as member deletion. For calculating the communication costs, most of the works compared considered different cases of group member addition/deletion in their proposed system. The authors in [83] considered a multi-group key graph structure for securing the unicast, broadcast and multicast communication in AMI. For both cases of joining/leaving, the number of keys that are updated depends on the position of the joining/leaving member in the multi-group key graph. The leave procedure has three cases: case 1 is when the user leaves his home DR project and is subscribed to only one DR project, case 2 is when a user

| TABLE I                  | NOTATION TABLE |
|-------------------------|----------------|
| Notation                | Description    |
| n                       | Number of smart meters |
| Np                     | Number of DR projects |
| n_j                     | Number of jth DR project member |
| Nsub(u_i)               | The number of DR projects to which user u_i subscribes |
| [K]                    | Size of the key in bits |
| X                      | Nsub(u_i) |
| Y                      | Np - Nsub(u_i) |
| c                      | log_2(Np) |
| h_k                    | Height of the new home DR project |
| h(·)                   | Height of the one-way function tree |
| C_p                    | Cost for bilinear pairing |
| C_m                    | Cost for the multipoint multiplication |
| C_e                    | Cost for the encryption function e |
| C_g                    | Cost for generating one key |
| C_f                    | Cost for evaluation of the one-way function |
| A                      | C_p + C_m |
| B                      | C_e + C_f |
| P                      | (4n + 5) + C_f |
| Q                      | 4nC_f |
leaves is home DR project but is subscribed to multiple DR projects simultaneously, while case 3 is when the user leaves one DR project which is not his home DR project. The communication cost for the join procedure occurs for two cases: the first is when a user joins his home DR project and the second is the joining of a new DR project by the user which is not the home DR project of the user. The authors in [84] also considered the various cases for the joining/leaving procedure of the members in the key graph structure similar to [83] for calculating the communication cost. Similar to [83] and [84], the authors in [50] also consider the same joining/procedure for calculating the communication cost. Taking one example from Table IV, the results reveal that the scheme MK-AMI performs better than the scheme eSKAMI in terms of communication cost.

Table V provides the storage cost for the different schemes. The storage costs are calculated for both MDMS and smart meters. While the storage cost for MDMS is the same for all the schemes except KMSCC, the same is also true for the storage overhead in smart meters, except the schemes, KMSCC and SKM. The authors [83] calculate the storage cost of their scheme based on the number of symmetric keys stored in the MDMS and smart meters. They also consider the individual keys, group keys and broadcast keys required for unicast, broadcast and multicast transmissions. Authors in [77], provided the storage cost for every device on the user side and evaluate that the storage cost does not increase with the number of devices on the user side in the AMI system. The storage cost is influenced by the increase in the number of DR projects. Similar to [83], the authors in [84] also consider the number of symmetric keys stored in the MDMS and smart meters for calculating the storage cost. In [35], the authors calculated the storage cost based on the number of keys stored in MDMS and smart meters, similar to that of [83] and [84].

We also discuss the pros and cons of the schemes compared in Table III, Table IV, and Table V. Authors in [83] proposed a scalable multi-group key management scheme that supports unicast, broadcast and multicast communications. The results of the scheme proposed in [83], produce low storage and communication overheads. The key management scheme proposed in [77] also supports unicast, broadcast and multicast communications in AMI. Due to insufficient key management, the scheme in [77] is not able to provide scalability and also suffers from packet loss during communication. In [50], the authors developed multicast key management by combining an adapted identity-based cryptosystem and one-way function tree approach. The storage overhead is enhanced in [50] due to the use of separate one-way function tree for every demand
response projects. Similar to [77] and [83], the work in [84] supports unicast, broadcast and multicast communications. The results of the work in [84] demonstrate that it induces low storage overhead without increasing the communication overhead. The scheme [84] is based on a multi-group key graph structure which supports simultaneous management of demand response projects for every consumer. The proposed structure scales to smart grids consisting of dynamic demand response projects, as well as caters to the constraints of smart meters with respect to memory and bandwidth capabilities. Authors in [35] proposed a scalable key management system for AMI in smart grids. The scheme supports the management of multiple and dynamic response projects concurrently for each consumer. But this scheme introduces extra communication overhead, compared to existing ones, such as, [50].

V. Open Research Issues and Challenges

AMI network is large-scale communication network comprising of utility companies, customers, and smart meters, across multiple smart grid domain. Regardless of the extensive research efforts for ensuring security in AMI reviewed in this survey, there remains many issues and challenges that form potential research directions. Critical issues, such as, consumer privacy, attack vulnerabilities, and standardization are highly correlated with the smooth operation of key management system of AMI in smart grids. This section presents some key areas related to smart grids, in particular with key management in AMI, that can be focused upon as future research ventures.

**Scalable Architecture:** A scalable and pervasive communication infrastructure is very much significant from the viewpoint of both construction and operation of a smart grid. A common feature of smart grid systems is that, a large amount of sensors are deployed over a wide area for implementing the complex monitoring and control functions. Therefore, one prime challenge in smart grid is how to build a scalable AMI communication architecture to handle the huge amount of data generated by those sensors. A smart grid communication infrastructure needs to provide scalability in terms of adding devices and services into it, as well as enhancing the real-time monitoring of energy meters. It is evident that conventional cryptographic solutions do not meet the requirements of a smart grid, in terms of scalability and efficiency. Therefore, we need scalable but secure and efficient schemes, tailored specifically for smart grid AMI communications. This will enable secure and efficient processing of meter reading data collection and message distribution management. Very few works, such as [45], investigated the scalability issue of distributed architecture in AMI. Also, key graph techniques can be used for addressing the scalability issue in AMI [35]. The proposed works considering scalable distributed architecture have shown promising outcomes with respect to key management of AMI. Therefore, future work should emphasize in building robust scalable distributed AMI communication architecture in smart grids.

**Content Centric Networking:** Content Centric Networking (CCN) is emerging as the fundamental paradigm for the future Internet and research initiatives are being undertaken for utilizing it further. CCN provides for paradigm shifting by deviating the focus of communication from the residing area of information to what information is needed. The advantage of CCN lies in the fact that it supports multicast mechanisms and deployment of in-network caching. Thus, information is targeted towards the hosts who are actually interested, rather than hosts with particular destinations. The in-network caching of data in CCN improves network quality of services, especially, delivery latency. The Content Centric Networking approach can be applied on AMI as a prospective future research area. Taking into consideration the caching advantage of CCN, it is widely believed that CCN can effectively reduce the AMI network bandwidth. So, CCN can play a major role in the traffic control development for the AMI system. The role of CCN in key management of AMI can be investigated to analyze how much effective role it plays.

**Defensive Mechanisms Against Threats and Attacks:** AMI in smart grids are very much exposed to several threats and other vulnerabilities. AMI is an appropriate example of cyber physical systems comprising of different types of hardware, communication devices and MDMS. Therefore, AMI is very much exposed to cyber physical attacks. Smart meter networks and MDMS software must have sufficient security to prevent any unauthorized modifications related to software configurations, recorded data readings, etc. Another prevalent attack of AMI in smart grids is Denial of Service (DoS) attacks. These attacks are related with temporary or permanent disruption of communication link and preventing message transmission/reception by flooding/jamming. In DoS attacks, an adversary may forge the demand request of a smart meter and keeps requesting a large amount of energy. Data integrity attacks also affect the normal operation of AMI by altering data timings and false-data injection. Thus, attacks that are very much prevalent in AMI need further exploration, specially with respect to key management and prospective solutions provided for defending such attacks.

**Consumer Privacy and Security:** Consumer privacy protection is a major requirement for present smart grid infrastructure [96]. For this, smart meters should be equipped with latest storage components having high security precisions. It should not be accessed by unauthorized persons. The encrypted meter data can only be decrypted by authorized personnel. The protection of consumers privacy can also be made possible by making the load patterns and signatures indistinguishable to unauthorized entities [68]. Research in the area of providing consumer privacy and security is going on and smart meter users need to be reassured that their data is secure. Also, there

| Scheme   | Storage Overhead                                      | MDMS | SM, |
|----------|-------------------------------------------------------|------|-----|
| SAMI [83]| $2 \sum_{j=1}^{m} (m_j - 1) + 1 \log_2 (|A|) + N \text{sub}(u_j) + 1$ |      |     |
| KMSCC [77]| $n + N_{dr} + 1$                                      |      |     |
| SKM [50] | $2 \sum_{j=1}^{m} (m_j - 1) + 1 \sum_{i=1}^{N_{dr}(u_j)} (\log_2 m_j + 1) + 1$ |      |     |
| eSKAMI [84]| $2 \sum_{j=1}^{m} (m_j - 1) + 1 \log_2 (|A|) + N \text{sub}(u_j) + 1$ |      |     |
| MK-AMI [35]| $2 \sum_{j=1}^{m} (m_j - 1) + 1 \log_2 (|A|) + N \text{sub}(u_j) + 1$ |      |     |
is limited research on AMI authentication and confidentiality of user data privacy and behavior that needs serious attention.

Efficiency: From literature, it is quite evident that key management system is an essential component for secured AMI in smart grids. The key management systems used in smart grids must be scalable from the point of view that such grids contain devices in massive scale that exist in hundreds of organizations. Further, key management must offer strong security in terms of authentication and authorization, inter-organizational interoperability and ensure the highest possible levels of efficiency to ensure that unnecessary cost due to factors such as overhead, are minimized. It is very much evident that new and highly efficient key management systems are needed.

Role of AMI in Smart Cities: AMI could become one of the defining aspects of the smart cities of the future. Its widespread adoption could lead to a major impact in the efficient functioning of smart cities. The impact could be, unlimited savings and greater ease of use for consumers at all income levels and suppliers of utilities, by harnessing real-time data collection and consumer consumption patterns. If smart cities of the future depend on wireless networks to meet their utility demands, they can expect lower costs and greater bandwidth. Wireless networks also have the capacity to collect data from devices that are digitally-dormant today, as the existing IoT has shown that virtually everything can eventually be connected to the grid. Future works can be done where the role of key management system of AMI in smart cities are mainly focused upon.

Standardization: Future smart grids must rely on the standardization for smart metering techniques to enable their smooth functioning. Currently, extensive activities are being performed in standardizing components and communication between components of the advanced metering infrastructure. Standardization forms an integral part for ensuring interworking between the different manufacturers and the AMI machineries. Therefore, several institutes are striving hard to achieve this goal. Nowadays, AMI uses a lot of Internet standards. For example, the application layer standards IEC 61968, defined by the International Electro technical Commission (IEC), developed the AMI’s common information model [97]. The XML and EXI standards were designed by the World Wide Web Consortium (W3C) committees for addressing the issues of end-to-end messaging and formats. Thus, the standardization factor needs much more attention to make interoperability achievable for communication and information of AMI in smart grids.

VI. CONCLUSION

In this survey paper, we focus on the studies that investigate the challenges and opportunities of key management systems in AMI. We provide a comprehensive survey of the key management system of advanced metering infrastructure in smart grid. We first give a brief introduction of the smart grid and introduce the fundamental concepts of advanced metering infrastructure that have emerged with the smart grid. Further, we briefly describe how AMI is vulnerable to threats and defensive solutions can be provided by using key management systems. Next, we elaborate on the role of key management system in AMI followed by the different communication architectures that have adopted the key management systems of AMI. Then, we surveyed the state-of-the-art-works that developed mechanisms for efficient use of key management system in AMI. Security analysis of the schemes dealing with key management system in AMI is presented followed by performance analysis of those schemes with respect to storage, communication and computation overheads. Finally, potential research directions for key management system of AMI in smart grid security are identified. This key management system analysis of AMI brings new and promising perspectives and methodologies for future research in smart grid.

REFERENCES

[1] D. Wu and C. Zhou, “Fault-tolerant and scalable key management for smart grid,” IEEE Trans. Smart Grid, vol. 2, no. 2, pp. 375–381, Jun. 2011.
[2] N. M. Pindoriya, D. Dasgupta, D. Srinivasan, and M. Carvalho, “Infrastructure security for smart electric grids: A survey,” in Optimization and Security Challenges in Smart Power Grids, Heidelberg, Germany: Springer, 2013, pp. 161–180.
[3] W. Wang and Z. Lu, “Cyber security in the smart grid: Survey and challenges,” Comput. Netw., vol. 57, no. 5, pp. 1344–1371, 2013.
[4] S. Khasawneh and M. Kadoch, “Hybrid cryptography algorithm with precomputation for advanced metering infrastructure networks,” Mobile Netw. Appl., vol. 23, no. 4, pp. 982–993, 2018.
[5] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, “A survey on cyber security for smart grid communications,” IEEE Commun. Surveys Tuts., vol. 14, no. 4, pp. 998–1010, 4th Quart., 2012.
[6] X. Fang, S. Misra, G. Xue, and D. Yang, “Smart grid—The new and improved power grid: A survey,” IEEE Commun. Surveys Tuts., vol. 14, no. 4, pp. 944–980, 4th Quart., 2012.
[7] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, “An efficient Merkle-tree-based authentication scheme for smart grid,” IEEE Syst. J., vol. 8, no. 2, pp. 655–663, Jun. 2014.
[8] R. R. Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar, “A survey on advanced metering infrastructure,” Int. J. Elect. Power Energy Syst., vol. 63, pp. 473–484, Dec. 2014.
[9] A. Mahmood, N. Javaid, and S. Razzaq, “A review of wireless communications for smart grid,” Renew. Sustain. Energy Rev., vol. 41, pp. 248–260, Jan. 2015.
[10] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, “False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey,” IEEE Trans. Ind. Informat., vol. 13, no. 2, pp. 411–423, Apr. 2017.
[11] D. Choi, S. Lee, D. Won, and S. Kim, “Efficient secure group communications for SCADA,” IEEE Trans. Power Del., vol. 25, no. 2, pp. 714–722, Apr. 2010.
[12] M. Barbieri, F. Fuschini, G. Tartarini, and G. E. Corazza, “Smart metering wireless networks at 169 MHz,” IEEE Access, vol. 5, pp. 8357–8368, 2017.
[13] European Union, “Directive 2009/72/EC of the European parliament and of the council of 13 July 2009 concerning common rules for the internal market in electricity and repealing directive 2003/54/EC,” Official J. Eur. Union, vol. 52, pp. 55–93, Jul. 2009.
[14] “Directive 73/EC of the European parliament and of the council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing directive 2003/53/EC,” Directive 73/EC, vol. OJL211, pp. 94–136, Aug. 2009.
[15] Smart Grid Project. Eurelectric and the European Commission’s Joint Research Centre. Accessed: Sep. 15, 2018. [Online]. Available: https://portal.smartgridprojects.eu/Pages/Map.aspx
[16] F. Rahimi and A. Ipakchi, “Demand response as a market resource under the smart grid paradigm,” IEEE Trans. Smart Grid, vol. 1, no. 1, pp. 82–88, Jun. 2010.
[17] “Monitoring report smart meter deployment and TOU pricing,” Ontario Energy Board, Carpi, Italy, Rep., 2011. [Online]. Available: http://www.ontarioenergyboard.ca/OEB/Documents
M. Erol-Kantarci and H. T. Mouftah, “Energy-efficient information and communication infrastructures in the smart grid: A survey on interactions and open issues,” IEEE Commun. Surveys Tuts., vol. 17, no. 1, pp. 179–197, 1st Quart., 2015.

Y. Yan, Y. Qian, H. Sharif, and D. Tipper, “A survey on smart grid communication infrastructures: Motivations, requirements and challenges,” IEEE Commun. Surveys Tuts., vol. 15, no. 1, pp. 5–20, 1st Quart., 2013.

Y. Yan, Y. Qian, and H. Sharif, “A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid,” in Proc. IEEE Wireless Commun. Netw. Conf. (IEEE WCNC), 2011, pp. 909–914.

Y. Kabalci, “A survey on smart metering and smart grid communication,” Sensors, vol. 10, no. 1, pp. 52–69, 2010.

European Union, Meter-ON Final Report: Steering the Implementation of Smart Metering Solutions Throughout Europe 2008. [Online]. Available: http://www.meter-on.eu/file/2014/10/Meter-ON%20Final%20Report-%202008%20draft.pdf

S. Finner and I. Baumgart, “Privacy-aware smart metering: A survey,” IEEE Commun. Mag., vol. 50, no. 1, pp. 126–133, Jan., 2012.

B. M. Khan, J. Fuller, and J. Attia, “Light-weight key distribution protocols for smart grid communications,” in Proc. IEEE Comm. Netw. Conf. (IEEE SmartGridComm), 2013, pp. 498–503.

M. Bennmalek and Y. Challal, “MK-AMI: Efficient multi-group key management scheme for secure communications in AMI systems,” in Proc. IEEE Wireless Commun. Netw. Conf. (IEEE WCNC), 2016, pp. 1–6.

S. Y. Obhrai, I. Kanda, D. Famolari, and S. K. Das, “A key management framework for AMI networks in smart grid,” IEEE Commun. Mag., vol. 50, no. 8, pp. 30–37, Aug. 2012.

J. Kamo, L. Qian, J. Fuller, and J. Attia, “Light-weight key distribution and management for advanced metering infrastructure,” in Proc. IEEE GLOBECOM Workshop, Houston, TX, USA, 2011, pp. 1216–1220.

K. Rahibe, M. M. E. A. Mahmoud, K. Akkaya, and S. Tonyali, “Scalable cross-layer reconfiguration schemes for smart grid AMI networks using bloom filters,” IEEE Trans. Depend. Secure Comput., vol. 14, no. 4, pp. 420–432, Jul./Aug. 2017.

R. Deng, Z. Yang, M.-Y. Chow, and J. Chen, “A survey on demand response in smart grids: Mathematical models and approaches,” IEEE Trans. Ind. Inform., vol. 11, no. 3, pp. 570–582, Jun. 2015.

A. Mohammadali, M. S. Haghghil, M. H. Tadayon, and A. M. Nodoshan, “A novel identity-based key establishment method for advanced metering infrastructure in smart grid,” IEEE Trans. Smart Grid, vol. 9, no. 4, pp. 2834–2842, Jul. 2018.

M. Bennmalek, Y. Challal, A. Derhab, and A. Bouabdallah, “VerSAMI: Versatile and scalable key management for smart grid AMI systems,” Comput. Netw., vol. 132, pp. 161–179, Feb. 2018.

W. Wang, Y. Xu, and M. Khanna, “A survey on the communication architectures in smart grid,” Comput. Netw., vol. 55, no. 15, pp. 3604–3629, 2011.

S. Bera, S. Misra, and J. J. P. C. Rodrigues, “Cloud computing applications for smart grid: A survey,” IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 5, pp. 1477–1494, May 2015.

N. George, S. Nithin, and S. K. Kottayil, “Hybrid key management scheme for secure AMI communications,” in Proc. 6th Int. Conf. Adv. Comput. Commun. (ICACC), vol. 93, 2016, pp. 862–869.

J. Zhou, R. Q. Hu, and Y. Qian, “Scalable distributed communication architectures to support advanced metering infrastructure in smart grid,” IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 9, pp. 1632–1642, Sep. 2012.

K. Sharma and L. M. Saini, “Performance analysis of smart metering for smart grid: An overview,” Renew. Sustain. Energy Rev., vol. 49, pp. 720–735, Sep. 2015.

N. Saputo, K. Akkaya, and S. Uludag, “A survey of routing protocols for smart grid communications,” Comput. Netw., vol. 56, no. 11, pp. 2742–2771, 2011.

I. Colak, S. Sagiroglu, G. Fulli, M. Yesilbudak, and C. Covrig, “A survey on the critical issues in smart grid technologies,” Renew. Sustain. Energy Rev., vol. 54, pp. 396–405, Feb. 2016.

T. Sauter and M. Lobashov, “End-to-end communication architecture for smart grid,” IEEE Trans. Ind. Electron., vol. 58, no. 4, pp. 1218–1228, Apr. 2011.

Z. Q. Wang, W. Yang, Y. Yang, and S. Shi, “SKM: Scalable key management for advanced metering infrastructure in smart grids,” IEEE Trans. Ind. Electron., vol. 61, no. 12, pp. 7055–7066, Dec. 2014.

P. Jokar, N. Arianpoo, and V. C. M. Leung, “A survey on security issues in smart grids,” Security Commun. Netw., vol. 9, no. 3, pp. 262–273, 2016.

T. W. Chin, S.-M. Yiu, V. O. K. Li, L. C. K. Hui, and J. Zhong, “Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid,” IEEE Trans. Depend. Secure Comput., vol. 12, no. 1, pp. 85–97, Jan./Feb. 2015.

A. Unkeitt, T. Voss, and H. Pohl, “Threat modeling smart metering gateways,” in Proc. Eur. Conf. Smart Objects Syst. Technol. (SmartSysTech), 2013, pp. 1–5.

A. Sikora, “Implementation of standardized secure smart meter communication,” in Proc. 35th Int. Telecommun. Energy Conf. Smart Power Efficiency, 2013, pp. 1–5.

A. Zoha, A. Gluhak, M. A. Imran, and S. Rajasegarar, “Non-intrusive load monitoring approaches for disaggregated energy sensing: A survey,” Sensors, vol. 12, no. 12, pp. 16838–16866, 2012.

S. S. Hosseini, K. Agbossou, S. Kelouwani, and A. Cardenas, “Non-intrusive load monitoring through home energy management systems: A comprehensive review,” Renew. Sustain. Energy Rev., vol. 79, pp. 1266–1274, Nov. 2017.

O. Alrawi, I. S. Bayram, and M. Koc, “High-resolution electricity load profiles of selected houses in qatar,” in Proc. IEEE 12th Int. Conf. Compatibility Power Electron. Power Eng. (CPE-POWERENG), Doha, Qatar, 2018, pp. 1–6.

S. M. Tabatabaei, S. Dick, and W. Xu, “Toward non-intrusive load monitoring via multi-label classification,” IEEE Trans. Smart Grid, vol. 8, no. 1, pp. 26–40, Jan. 2017.

K. Wong et al., “An extensible approach for non-intrusive load disaggregation with smart meter data,” IEEE Trans. Smart Grid, vol. 9, no. 4, pp. 3362–3372, Jul. 2018.

Powerley. Powerley: Utility Designed Energy Management Solution. Accessed: Jan. 26, 2019. [Online]. Available: https://www.powerley.com/platform/

J. Liu, Powerley Unveils Energy-Driven Smart Home Experience. Accessed: Jan. 26, 2019. [Online]. Available: https://www.asmag.com/showpost/26733.aspx
