European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 05, 2020

Privacy, Data Management And Access Control In Smart Meters: A Survey

Rentachintala Kasyap[1] Dr.M.Murali[2]

[1]*M.Tech student, Dept.of Cloud Computing, SRM Institute of Science and Technology, Potheri, SRM Nagar, Kattankulathur, Tamil Nadu, India*
[2]*Associate Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Potheri, SRM Nagar, Kattankulathur, Tamil Nadu, India*

Abstract
Smart meters are automated devices that can exploit to monitor the real-time electricity consumers' power consumption. The smart grid with key technological enablers are considered as the collected information consumption that would useful for enabling the real-time schemes of new sophisticated billing. A wide-variety of value-added services could rise and the power distribution system's efficient operations could facilitate. As the meters can collect the consumers' sensitive data, the information of energy consumption is provided. For data collection, a prime challenge and a major concern is considered as privacy. In this paper, the metering data with different applications in the smart grid and the reviewing of relevant privacy legislation are made. The research implications, suggestions, structured overview, and defects of security solutions have been demonstrated for effective management and data delivery of privacy-preserving meter data. To collect the meter-data for three application areas such as 1) value-added services; 2) operations; and 3) billing including demand response, recent works on privacy-preserving technologies for collecting meter data have been investigated in this paper.

1. INTRODUCTION

The automated meters and smart meters include in the key enablers of smart distribution grids. For a device, the automated meters have been implemented to (i) Determine the consumption of electric energy using a variable time granularity and (ii) make a report on the computed consumption to a Meter Data Management System (MDMS). Additionally, automated meter is also called as a smart meter as it has a capability to (iii) receive the commands of direct load control or pricing data and (iv) make the information exchanging with the smart home appliances which optimizes the energy utilization and participates in demand response. A subset of smart meters is the control functionality and data collection of automated meters. A subset of issues relevant to smart meters is to the subset of privacy issues relevant to automated meters.

In most of the countries, the metering systems can store and transmit the information of measured data at time intervals of 15 minutes. But, it's common that the reporting hourly and daily.

Based on the population density and country, the utilization of communication technology is varied. However, the most common technologies are involved ZigBee [1]. Power-Line Communication (PLC), and cellular networks. Often, the information is delivered by using a hierarchical model and is processed at medium or low voltage substations. Over an IP

network, the data is delivered to the MDMS. From the premises of customers, the information could be transmitted through the 'public' communication networks (non-dedicated) like the Internet.

The infrastructure of smart metering in different domains subsuming the meter data management, communications, customer domain, and different services based on the metering data are illustrated in Figure 1.

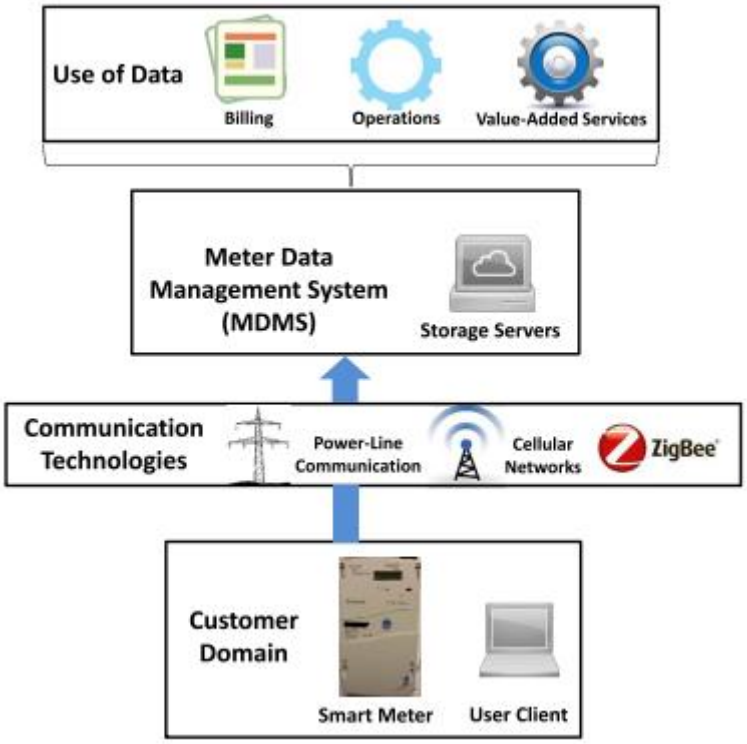

Figure1: Different domains of the smart metering infrastructure

A. Operations, Billing, and Value-Added Services

In a smart grid, one of the many sources of information is considered as an automated and smart meters which can collect the measurement data and can use in integration with other collected information sources using actors that involve the operators of smart grid and distribution system, electricity markets, bulk generation, and the transmission system operator. In three different types of tasks, the measured data can be used such as operations, billing, and value-added services. Significantly, these are differed in required information about number and locations of consumers, requirements on accuracy and frequency of metering data, and the stakeholders.

*Billing***:** In the dynamic pricing, the accurate customer billing is the usage of automated meter data. The consumption of information is not required to perform in real-time owing to the monthly-basis processing of billing but accurate time of using information and accurate measurement data are require in the correctness of billing.

*Operations***:** The smart meter data can also be used to achieve the improvement in reliability and efficiency of electricity distribution specifically in the distributed generation. Because of the distributed generation [2] automated meter data can use by utilities to parameterise the intelligent Feeder Protection Systems (FPS) at substations in the back-feed availability or to improve the integrated Volt and Var Control (VVC) and State Estimation (SE) of distribution

system [3], [4] For detection of faults and achieving the improved automated Fault Location, Isolation, and Service Restoration (FLISR), the meter data can also be used by them. The real-time or near real-time data processing are require for metering data but with possible different measurement accuracy and different granularities. The individual meter data may require for FLISR to identify the fault location, make the restoration planning, and island control while VVC, SE, and FPS may operate using aggregate meter data from a feeder section or a feeder.

To improve the demand forecasts, smart meters could be utilized that deliver the information from smart appliances beyond the ancillary and reliability services. For example, the future power demand could advertise by an already active appliance or programming of an appliance is accomplished to be moved in an active state at a certain time that the expected curve of power demand could advertise as a dynamic pricing function. The utilization of demand response can be enabled by the smart appliances' controllability and demand forecasts for ancillary services that means an operator can allow for reducing the demand through the appliances switching-off while in the supply scarcity. The information of real-time demand requires in such real-time direct demand response.

Value-Added Services: To provide value-added services, smart meter data could leverage by operators, consumers, and third-party service providers. These services are for the electric appliances diagnostics and for the management. Based on the third-party business model, value-added energy services could provide for a fee or for free and the transformation of the electricity market could accelerate [5].

Based on the provided guidelines for economic demand response i.e. the demand scheduling as a function of the predicted prices of electricity, management services can use to reduce the consumers' energy bill. The appliances like dishwashers, washing machines, and home or building energy management systems involving Heating, Ventilation, and Air Conditioning (HVAC) [6] could include in the controllable loads. In order to achieving energy savings, economic demand response could provide using a service provider of energy management. The coordination of demand response services of economic and ancillary could process and allow the customized tariffs in the ancillary demand response programs with the consideration of customers' engagement.

For detection of anomalous consumption patterns like appliances that consume excessive energy or appliances that terminate the end of life cycles, consumers can make use of diagnostics and maintenance services. These services could implement based on the correlation of consumers' data consumption with similar profiles without regarding the proximity [7]. For the lifecycle management of products, a free service may provide by an equipment vendor in return for statistical information.

I. Automated and Smart Meters Collect Personal Data

For an unintended and fourth purpose of invading the privacy of consumers, smart meters and automated meters are collected the information. Based on the load signatures [8], a significant recent work shows that the individual appliances can detect from the traces of energy consumption with detailed analysis [9]-[10] [11]. To infer a household's occupancy and to invade the consumers' privacy, frequent meter readings and data mining algorithms can also be used in more sophisticated ways respectively based on the revealing the economic status and life-styles [4]-[8]. The interests of consumers could also reveal by recent work that shows enough measurements. From the profile of electricity usage, the displayed TV channel can be estimated for a sampling period of 0.5 s by Greveler et al. [16]. For the smart grid, a

data governance framework tailor-made is called as the privacy is considered as a serious concern.

Ref.no	Author name	Proposed work	Importance
1	DM. Han et al., (2010)	Different home network tasks are divided and assigned to appropriate components using the proposed smart home energy management system. By supporting the active sensor networks that has both actuator and sensor components, diversified physical sensing information can integrate and control different consumer home devices using proposed system. To improve the ZigBee sensor networks' performance, a new routing protocol DMPR (Disjoint Multi Path based Routing) is developed.	Because of flexible integration into everyday life, widespread attentions have been gained by the Smart home energy network. Various home appliances, wireless communication technologies, and smart sensors are unified by this next generation green home system transparently.
2	Jouni Peppanen et al., (2015)	The intelligent methods are presented by the author to detect and deal with the inaccurate or missing smart meter data and ways to process the information for various applications. The method of an efficient and flexible parameter estimation is also presented based on the regression analysis and voltage drop equation for improving the distribution system model in terms of accuracy. A 3-D graphical user interface is presented for visualization of the system state and events with advanced version.	At the distribution system level, the various new distributed energy resources being installed that need increased visibility into system operations. It will enable using situational awareness applications and distribution system state estimation (DSSE).
4	PA. Pegoraro et al., (2012)	Based on the consideration of characteristics variable over loads time and generation from renewable sources, the investigations are extended to the optimal meter placement. Under the uncertain and time variying behaviour of the renewable generation and loads, the given constraint of accuracy is able to achieve by the distribution system state estimation (DSSE).	For an effective operation and control, a critical element is the design of measurement infrastructure for future active distribution grids. A new paradigm is provided for the system of distribution grid monitoring using the real-time and accurate measurements from heterogeneous existing and emerging metering devices.
5	CE	To use new sources of transparent	To accelerate the market

	Kontokosta et al., (2013)	and available information publicly, a framework is outlined the significance of energy disclosure requirements. The mechanisms are presented through which information can change market behaviour in the commercial real-estate sector and a wiring diagram is developed for the information flows based on the establishment of data ecosystem.	transformation around building energy efficiency, one of the most promising public policy tools is represented using energy disclosure laws.
6	Korosh Vatanparvar et al., (2015)	For monitoring and controlling all of the appliances in a house, a novel HEM platform is presented that uses a low power IEEE 802.15.4 standard. To implement the monitoring and controlling algorithms, Service-Oriented Architecture and Devices Profile are used for Web Services. The flexibility and scalability of the platform could improve. In this platform, some other features also implemented such as open-source architecture, remote access feature, and plug-n-play capability.	For improving the energy usage in the residential buildings, Home Energy Management (HEM) may be utilized. The time-to-market and making the HEMs hard to penetrate the consumer market have increased with the scalability, cost, and flexibility of hardware and software available architectures.
11	Michael Zeifman et al., (2012)	Based on the individual appliances and/or end users, a new approach proposes for disaggregation of electricity consumption and it would improve the home energy displays in terms of effectiveness.	The emerging home energy management devices are considered as home energy displays. Due to the higher consumption of data for the display whole-home electricity, the potential of energy savings is limited.

Privacy Legislation for Smart Meter Data

Based on the foreseen provisions for "personal data", the smart meter data must be managed as a consensus. An opinion about the smart meters' data usage is issued by the European Data Protection Supervisor. In smart metering or smart grids, it is stated that the stakeholders should be aware that the personal data processing will obey with the national legislation transposing fully subsuming Directive 95/46/EC, and to the applicable extent for the e-Privacy Directive.

Until the law is allowed selectively, the personal data collection is forbidden based on the current policy of EU. The explicit legitimation is included that indicates the data is necessary to achieve the specific purpose if the personal collecting entity can demonstrate the information. To preserve a societal interest like the power grid stability, the smart metering data is require which could describe by a Distribution System Operator (DSO). The limitation of purpose is limited by the collection of personal data even it is allowed. The collected

personal data can't be utilized for a different purpose like profiling and for only one particular purpose like billing. A separate legitimation is required for every additional purpose.

Although the provided guidelines of NIST on privacy aspects in 2010, federal regulation is not placed on the privacy of smart meter data in the U.S. [14]. By making the landscape instead of inhomogeneous and fragmented, additional regulations have been built in California and other states [15]. According to the guidelines similar to the EU legislation, the U.S. Department of Energy [16-17] was released a voluntary code of conduct for third parties and utilities for addressing this deficiency.

Two Notions of Privacy

For privacy, the legal framework includes two different fundamental notions and heterogeneous characteristics in the literature.

Cryptographic privacy: Based on the results from an algorithm, the information can be learned is limited to the leaked data by an algorithm which require in cryptographic privacy [18]. The information can learn from the result of algorithm be limited by the leaked information of an algorithm that requires in cryptographic privacy [18].

Statistical privacy: In statistical privacy, an algorithm's result (possibly randomised) that executes on a data set must not be disclose sensitive data relevant to the individuals. Here, the main goal is to restrict the possible set of inferences according to the result. In statistical privacy, a well-known notion is the differential privacy notion that requires to be similar to the algorithm's result while executing on same data sets. For adding or removal of a consumers with a probabilistic sense [19], aggregation must be insensitive. At least k-1 other consumers should be available for other consumers whose information contains in the aggregate for each consumer include in an aggregate and are indistinguishable for privacy's another notion is kanonymity [20]. To describe the statistical privacy axiomatically including differential privacy, refer to [21].

It's essential to consider that the focusing of privacy with two notions is balancing. Two queries of consumption information about electricity is considered for describing the difference. The anonymised hourly data of households' electricity over a year would be requested by the first query. The second query would consider the durations and blackout locations over the course of the same year. The attacker receives the anonymised information would be ensured while computing the two queries based on the guaranteeing of cryptographic privacy. But, the two queries results could be linked by the attacker and the inferring of consumer locations or identities based on matching blackout events with the reduced consumption of electricity in the household.

It's very important to achieve both privacy notions for protecting the private information. If attackers can manipulate the information of protocol and data and can collude, this is even more and it results in the defining of attacker models and requirements of security.

Requirements for Management of Smart Meter Data using Privacy-Preserving Protocols

- *Authenticity:* The data relevant to the source should validate by the receiver of meter data.
- *Confidentiality:* While transmission of information (data-in-transit), computing (data-in-use), and storage (data-at-rest), meter data should not be exposed for unauthorized processes or individuals. To achieve the cryptographic privacy, the confidentiality of data-in-use, data-at-rest, and data-in-transit is required to be ensured.

- *Auditability:* The possibility of verifying whether the response to a request (computation on meter data) should be made.
- *Non-Repudiation:* As the source of meter data initiates the data, it shouldn't be able to deny that implies the integrity and authenticity.
- *Integrity:* The maintenance of meter data should be done with correctness and accuracy and should have to detect any occurred changes to the data during computation, storage, and transmission.
- *Authenticity:* The source of the data should be verified by the meter data receiver.

By preserving the privacy that relies on the attacker model significantly, it's a challenging task for achieving the requirements of security. The assumption of following the protocol honestly is considered under the honest-but-curious (also called semi-honest). For example, this model doesn't manipulate the data. From the protocol, the attacker can deviate and modify the protocol messages in the model of malicious attacker. Various meters may control by a malicious attacker or may pretend to have multiple identities. This could be the best example of a Sybil attack.

Two additional security requirements can formulate that related to the solutions for integrating the data from multiple meters and to address malicious attackers.

- *Non-Malleability:* Without involving in the detection process, the alteration of encrypted data shouldn't be accomplished by an attacker.
- *Sybil Attack Resistance:* For meters that include multiple identities, the solution should be resilient.
- *Byzantine Attack Resistance***:** For colluding meters, the solution should be provided without compromising the robustness. For example, meters have been compromised.

Ref.no	Author name	Proposed work	Importance
14	Marek Jawurek et al., (2011)	Without disclosing the actual consumption profile to the supplier, the billing with time-of-use tariffs is enabled using a proposed privacy-presreving protocol. Based on the commitments of Pedersen processed using a plug-in privacy component, the approach depends on a zero-knowledge proof that is put into the communication link between the back-end system of supplier and Smart Meter. No changes require to the hardware of Smart Meter and small changes only considered for the software of back-end system and Smart Meter.	In households of customers, the replacement of traditional electricity meters is done with Smart Meters which collects the profiles of fine-grained utility consumption from consumers. It leads to the enabling of introducing time-of-use and dynamic tariffs.
15	Arik Friedman and Assaf Schuster (2010)	To build the algorithms of privacy-preserving data mining, a naïve utilization of	Based on the framework of differential privacy, a data access interface is given

		interface is presented that could results in the inferior data mining. This issue is addressed with the consideration of algorithmic requirements and privacy simultaneously. As a sample application, it is focused on decision tree induction. The chosen methods using the data miner performance has been impacted profoundly by the privacy mechanism. This choice could differentiated the accurate classifier and a completely useless one.	for the issue of data mining with formal privacy guarantees. In any specific record of an individual, the changes are insensitive by the computations which require for differential privacy.
16	Latanya Sweeney (2002)	To achieve fc-anonymity, a formal presentation of integrating suppression and generalization is provided. Here, generalization includes replacing or recording of a value with a less specific but constant value semantically. A value is not released in suppression. The Preferred Minimal Generalization Algorithm (MinGen) which presents a theoretical algorithm. Here, these techniques are integrated to offer the protection of fc-anonymity with minimal distortion. Additionally, the comparison of MinGen with the real-world algorithms like Ji-Argus and Datafly is made.	The person-specific records are require to share by data holder such as a bank or hospital in a way that the individual's identities can't be determined. Here, the individuals are the data subjects. The released records adhere to kanonymity is one way to achieve this. That means, at least (k-1) other records has included in each released record and the values of records are unclear over the fields display in external data.
17	Stephen McLaughlin et al., (2009)	Through the manipulation of AMI systems, consider the adversary by means of defrauding the electrical grid. By processing the penetration testing on commodity devices, manipulate the energy usage data and verify these attacks viability using the methods adversaries. In AMI systems, the theft is still possible through these activities and a myriad of new vectors are	A new computerized "smart grid" is transitioned by global energy generation and delivery systems. An advanced metering infrastructure (AMI) is one of the significant components of the smart grid.

		introduced for achieving it based on the current AMI devices.	
18	Muhammad Rizwan Asghar et al., (2013)	For the smart grid and its relevant privacy legislation, metering data is utilized for different purposes. The structure, recommendations, drawbacks, and research directions for security solutions require for privacy-preserving meter data management and delivery are provided. To collect the meter data for three applications areas: 1) value-added services, (2) operations, and (3) billing subsuming demand response, privacy-preserving technologies have been considered.	For monitoring the energy consumption of electricity consumers, automated and smart meters are used in near real-time. These are considered as the smart grid's technological enablers significantly. It could enable new schemes of sophisticated billing which provides efficient operation of power distribution system.

Consent and Access Control

For private information using by each an individual, explicit consent provides by consumers as mentioned in Section III-A. The explicit consent would need from the consumer although it provided by the same entity along with the standard uses like operations and billing and further value-added services. Therefore, it's important that sufficient data has available for consumers to make decisions informatively relevant to the regulation of an access to the private data for enabling the services of a third party [22]. Typically, the MDMS would enforce such type of access control decisions.

The requested data should be able to access by an authorised entity principally and the least privilege principle is followed [23]. Different types of access control mechanisms such as Role-Based Access Control (RBAC), Discretionary Access Control (DAC), and Mandatory Access Control (MAC) [24]. The eXtensible Access Control Markup Language (XACML) is offered the policies of flexible access control [25], [26]. Since we are moving from coarse-grained to fine-grained access control, the challenging task is that the flexible access control owing to the involvement of policy specification with more complexity and incurring significant overhead. In a similar manner, private data about the sensitive information might reveal by access control (e.g., [24]) specifically in case of enforcing the access control policies in untrusted or semi-trusted environments. In [27], a solution is demonstrated to limit the private data in semi-trusted environments where the policies of encrypted role-based access control have been used. An incurring of a high computational overhead is done. For expressing the policies of consent and access control that would use in the smart grid, the specification language (usable) problem is used and it is still not determined.

It's technically challenging task that the accessing of private data for a specific purpose although a specification language existed. Whether the information is processed based on the given consent or not, existing solutions can't be verified although a consent is provided (as mentioned in [22]) for a private data with a particular use. It becomes an open issue of

verifying the processing of data based on the given consent and enforcing the expressive policies with scalability and efficiency. To ensure the privacy, a common approach is used for manipulating the information rather than verification so that it can be utilized for particular purpose that permits the access. In section V, such type of solutions will be discussed.

D. Data Integrity and Auditing

Based on traditional cryptographic solutions like PKI-based approaches [28], both for storage and communication [29], data integrity ensures as it is essential for accurate metering. From a perspective of privacy, it's very problematic to protect the data integrity based on schemes like PKI because it can expose the consumers' identities for third parties such as storage providers. Specifically in untrusted and semi-trusted environments [30], [31], one may have to depend on approaches of anonymous authentication to protect the information of identity. The problems of revocation and efficiency could be faced by the anonymous authentication.

Auditing is an essential problem relevant to integrity, i.e., whether the correction of received in response to a request or not is verified. A challenging problem is that the auditing data without invading privacy while various solutions are existed for the auditing issue in general [32-36]. To validate the cost of consumption, the recent schemes allow consumers not disclosing the data consumption to the MDMS [37-38], [41]. According to the commitments [39], these schemes are implemented and aggregators are honest-but-curious, i.e., they are true while making computations like verification of digital signatures but are curious in learning the consumption of data. The computations verification made using the aggregators do not support by these solutions. Under privacy requirements, the public auditing of stored data is becoming a related problem that means the metering data of a consumer is verified using a third party without invading the privacy. By using a public key-based homomorphic linear authenticator, a solution was proposed in [40] for auditing the encrypted data publicly on cloud storage. It's not clear that whether such type of a solution is suited for smart grids to audit the metering data on real-time by considering the producing of data continuously as the choosing of solution is made randomly using the data blocks verification. Based on the intended use of the data, the real-time constraints are given for operations.

Ref.no	Author name	Proposed work	Importance
23	MR Asghar, G Russello (2012)	For managing the consent, ACTORS are presented with a goal-driven approach by the author. The goal-driven approach of Teleo-Reactive (TR) programming is leveraged with the use of ACTORS for management of consent by considering the changes relevant to the contexts and domains where the patient provides his/her consent.	The capability of revoking and granting the consent with efficiency is empowered by this proposed work. Based on the situation of a patient, the process of revoking and granting is varied greatly.
24	JH Saltzer, MD Schroeder (1975)	The author describes the proposed method in three main sections. Section I includes the examples of elementary protection and authentication mechanisms, design	From unauthorized use or modification, the computer-stored information is protected using mechanics. For

		principles, and desired functions. The first section should found to be accessible if any reader familiar with computers. Section II examines the modern protection architectures and the relation between access control list systems and capability systems principles with detailed analysis. Additionally, it ends with protected objects and protected subsystems with a brief analysts. To understand this section, some knowledge about descriptor-based computer architecture is required.	supporting the information protection, those architectural structures are considered -whether software or hardware.
25	R.S. Sandhu et al., (1996)	As a method of security administration and review, the author focuses on describing why role-based access control (RBAC) is receiving renewed attention. A framework considered with developed four reference models to understand RBAC in a better way and categorizes various implementations and discusses the RBAC utilization for managing itself.	A role-based access control approach utilizes to simplify the complexity of security administration of large systems.
31	Jan Camenisch et al., (2006)	A credential system creates by the author that allows a user to authenticate anonymously at most n times in a single time period. A dispenser of n e-tokens withdraws by a user. For authentication, an e-token is used to a verifier. Each e-token can utilize only once. For each time period, the dispenser refreshes automatically. To this problem, the prior solution is that the protocols are a factor of k slower for the verifier and user. Here, k represents the security parameter.	Basically, Glitch protection designs for hones users who reuse e-tokens occasionally. A reused e-token can recognize by the verifier. The anonymity of users preserves and they don't reuse e-token too often. \
32	Patrick Tsang et al., (2008)	A new anonymous authentication scheme proposes known as PEREA. Here, the bottleneck computation is *not rely on the size of the revocation list*. Instead of time complexity in authentication is linear in the size (K << L) of a *revocation window*, the number of	To make future accesses, various authentication schemes used that allow servers to revoke the ability of misbehaving users. These schemes rely on powerful TTPs that are having an ability

		subsequent authentications is considered if in case the user is revoked after recognizing the misbehaviour of a user. The security of construction proves and a prototype implementation of PEREA have improved to validate the efficiency experimentally.	of deanonymizing the users' connections (linking).
34	Hwee Hwa Pang et al., (2005)	A scheme introduces by the author for users to validate the query results are authentic (i.e., all values initiate from the owner), and complete (i.e., omitting no qualifying tuples). The proposed scheme gives a support for the selection on non-key and key attributes as well as the queries on relational databases. The access control policies comply with the scheme as it is computationally secure and can be developed with efficiency.	In publishing of data, the satisfying user queries role delegates to a third-party publisher by the owner. Incorrect queries could produce as the publisher may be susceptible or untrusted to the attacks.
37	Michael Backes et al., (2013)	To determine the solution for issue of computations class of quadratic polynomials over a large number of variables, the novel cryptographic techniques propose. Notably, a wide range of arithmetic computations with many important statistics cover in this class. The encouraging performance results show to retain the solution efficiency. For example, the size of below 1 kB have included the correctness proofs and are validated based on clients less than 10 milliseconds.	A large amount of data with an untrusted server stores by a client to address the problem. The storage is done in a way that the client can ask the server at any moment for computing a function on the outsourced data with some portion.

II. The non-trusted operator model implements for service-specific privacy protection

The utilities, operators, and value-added service providers are considered as non-trusted entities which is alternative to the trust model mentioned. The large number stakeholders are inspired by this trust model and their business models and interests are not known to consumers as they involve in the smart grid ecosystem. The privacy of consumer has ensured with the use of a model of non-trusted operator that includes the meter data computation in a way that they can utilize for different purposes such as operations, billing, and one of many value-added services. It's essential to consider the meters security to preserve the privacy under this trust model although we don't describe here.

Privacy-Preserving Billing

In dynamic pricing, the accurate billing is the major advantage of automated metering arguably. To enable correct billing, the changes in electricity prices frequently require for detailed information about consumption of energy is the significant challenge in privacy-preserving billing. But, the private information may lead with the detailed information about energy consumption (ex: one reading every 15 minutes).

A. Secure Computation for Cryptographic Privacy:

The energy suppliers are enabled with the use of alternative approach for preserving the privacy of customers by computing the bills without accessing for any individual readings. Jawurek et al. [41] was proposed a scheme using Pedersen commitments with the introduction of a privacy component inserted into the smart meter to restrict the privacy leakage. This scheme allows the sending of billing information to the energy supplier based on the signed commitment. The smart meter is used to sign on the commitments and the energy supplier for verification of data. Rial and Danezis et al. [43] were focused on extending the context of calculating the bills under a tariff of non-linear consumption. The solution is depended on the integration of the Non-Interactive Zero-Knowledge proof (NIZK) [43] and integer commitment of Groth, and on the generalized anonymous credential system of Camenish and Lysyanskaya [44]. A solution is also proposed by them to make the billing process under an affine consumption tariff without relying on the NIZK. The power demand with instantaneous data i.e. the necessary data for operations couldn't be received by the energy supplier that is the drawback of these schemes.

Molina-Markham et al. [45] was considered a different technical solution conceptually with the implementation of a zero-knowledge protocol. The smart meter can act as a prover in the proposed architecture and the power such as gas, electricity, or water is considered as a secret. It is intensive computationally owing to the limitation of its wide scale adoption since the solution is relied on homomorphic encryption and a zero-knowledge protocol.

For supporting the operations like voltage control, any solution is not provided that could inform the operator regarding the instantaneous power demand beyond the number of proposals using a non-linear consumption tariff for billing of privacy-preserving and the solutions using an on-site battery. The value-added services may not feasible with the battery-based solutions. For example, monitoring of anomalous consumption patterns.

B. Privacy-Preserving Operations

Essentially, the secondary usage of smart meter data is that the ensuring of safety and improving of operational efficiency in distribution grids. The individual smart meter data may not require in enhancing the operations not similar to the billing. To know the aggregate power supply instantly, it may be sufficient and the power supply is within the power network areas. Based on the application, the area size and the aggregation level is performed. For example, district, substation, neighbourhood, or an entire city. The level of privacy protection is influenced by the number of aggregated consumers and it may impact on the operational efficiency in case of system identification [46], or distribution state estimation [47], [48].

1) Cryptographic Privacy using Aggregation Algorithms: There are various literatures available for cryptographic privacy based on aggregation algorithms with and without inclusion of a trusted third party. Most of the researches are focused highly on the privacy-

preserving aggregation and little attention towards the trading-off between the data usefulness and privacy-preservation to improve the efficiency in operations.

a) In case of a trusted third party: For meter data with privacy-preserving aggregation cryptographically, different solutions develop using a trusted third party [49]. Efthymiou and Kalogridis [49] were demonstrated a scheme to anonymise the metering data by considering an assumption of a trusted escrow service for aggregating the smart meter data. For billing, each smart meter includes a profile of non-anonymous client data with the utility. In the proposed solution, the aggregation of data from various meters accomplishes based on an anonymous data profile that embeds the escrow services. Bohli et al. [50] was proposed a solution in which the consumption data of consumers is aggregated in a neighbourhood and is sent to the energy supplier. The aggregation consumption per consumer is also submitted by the solution at the ending period of each billing but time-of-use pricing doesn't allow here. The transmission of solution is to the neighbourhood gateways merely in similar to [49]. The possibility of approaches with a notable weakness that relies on a trusted third party which being compromised and a solution is required in such a way that it can allow the operators or customers for identifying the trusted third-party with any compromise in real-time.

b) Not involving a trusted third party: Either using designed channel codes for the wiretap channel or using some form of homomorphic encryption, solutions are implemented without involving the trusted third party that rely on secure multi-party computation [51]. To process the operations over encrypted data, non-trusted third parties are allowed by homomorphic encryption. Without declining the accuracy of results, the third party could implement any number and combination of arithmetic operations ideally (ex: division, multiplication, subtraction, and addition) on the encrypted information. However, it's very difficult to achieve. The algorithms of state-of-the-art homomorphic encryption are involved within one of two categories such as fully homomorphic cryptosystems and partially homomorphic cryptosystems. Exclusively, a partially homomorphic cryptosystem provides either multiplication or addition. The partially homomorphic cryptosystems has included the examples of Benaloh [54], the Goldwasser-Micali [53], and the Paillier [52] that support addition. The examples of partially homomorphic cryptosystems supporting multiplication are included RSA [56], and ElGamal [55]. Both addition and multiplication are supported by fully homomorphic cryptosystems unlike partially homomorphic cryptosystems. Such type of cryptosystem [57] is not yet practical because of the occurrence of high computational overhead that retrieves by cryptographic system's underlying operations.

Based on decentralized, centralized, and distributed architectures, the exploring of additive partially homomorphic cryptosystems utilization has presented without using a trusted third party model. By using the Paillier cryptosystem, the aggregation of consumption data is done at network gateways in EPPA [58]. Ruj and Nayak [59] were introduced a solution with the use of Paillier cryptosystem based on the integration of attribute-based encryption. Here, the aggregation of data done in a hierarchical way based on network elements like home area gateways, remote terminal units, and building area gateways. Li et al. [60] consider a scheme wherein smart meters are connected in a form of mesh network and data is aggregated by themselves with the use of Paillier cryptosystem. The most common point between these works is that the meters are considered as honest but curious and not concerning the malleability. Vetter et al. [61] describe an architecture which encrypts the data rather than aggregation of information based on a partial homomorphic cryptosystem which allows the encrypted values' aggregation and the encryption keys aggregation. By using the aggregated encryption key, the decryption and querying the aggregated data can perform with the energy

provider and the encrypted data stores in a database grouped by region. In case of known-plaintext attacks, this scheme is not secure.

In [62]-[63], solutions were considered based on asymmetric and symmetric DC-Nets. Chaum [64] was introduced the DC-Nets to compute the secret or Boolean values by relying on a temporary secret shared among participants. They can provide unconditional privacy but showing sensitivity for disruption attacks, i.e. the results of the computation not useful by rendering a malicious attacker. Aggregation protocols were introduced based on DC Nets that include a low overhead aggregation protocol which allows the building of shared secrets based on public keys.

The permanent private keys are used for encryption by participants in asymmetric DC-Nets [65] in contrary to the symmetric DC-Nets of Chaum. The sum of private keys is used in the aggregator which assumes that the recognition of decrypting the aggregate value. Unconditional security or perfect forward secrecy do not provide by asymmetric DC-Nets but the aggregator is allowed for verifying the individual values and the aggregated value at the price of sacrificing privacy. The solutions are considered based on asymmetric and symmetric DC-Nets and made an argument that asymmetric DC-Nets are generalised the solutions with the use of partial homomorphic cryptosystems. When compared to symmetric DC-Nets that require addition or XOR, more complex cryptographic primitives like multiplication and exponentiation require in asymmetric DC-Nets.

The solution is presented based on wiretap codes for a secure multi-party computation scheme that doesn't rely on the homomorphic encryption. It allows the computation of linear functions for distributed data in a network and an overhead has included that linearly grows in the number of meters.

2) Facilitating Statistical Privacy: In case of Sybil attacks, the potential vulnerability is an essential issue for the solutions using multi-party computation, i.e., colluding meters whose focused on achieving the revealing of private data of other meters. By using the differential privacy notion, a number of privacy-preserving aggregation schemes have been evaluated and formulated that are robust against colluding meters. With the addition of random noise to the measurement data, widespread use in solutions has been found out for privacy-preserving aggregation without the inclusion of a trusted third party [66], [67], [68].

Bohli et al. [66] was made a conclusion of achieving the desired level of differential privacy under the assumption of normally distributed noise. It would require much large groups of aggregation for the practical solution. In [67], the Laplace distribution was used which is the most popular distribution for the noise that helps to devise a protocol that depends on exchanging of information between the meters. The protocol is operated robust for faulty nodes but the data may irrecoverable with the malicious meters.

To achieve the differential privacy, the most crucial aspect is that the potential effect of the noise on applications of smart grid such as state estimation, VVC, and dynamic relay configuration. The trade-off between accuracy of state estimation and differential privacy under Laplacian and Gaussian noise on a single feeder is quantified as a first step in the recent works [68]. It's unclear that they are general in numerous applications FLISR, VVC, and optimal power flow if generalisation of results can be done for topologies.

The existed algorithms give an access for disclosing a power consumption time series without an attacker in real-time for leveraging the temporal correlation between subsequent samples is another critical aspects of achieving the differential privacy with the addition of random noise to invade the privacy. In [69], an approach was proposed based on adaptive sampling

and filtering for traffic and epidemic data. But, it's not clear that the consumer privacy would preserve by such approach when applied to smart meter data. Finally, we can't determine whether the possibility of adding random noise in such a way that it doesn't impact on the billing correctness.

3) Privacy Economics: To share the frequent reading of meter data with the operator, an alternative approach would be considered for aggregation to provide an economic incentive to customers. By relying on the activities sensitivity, time-of-day, and the financial incentive, each customer would be allowed to take a decision regarding the reporting frequency on an individual using a market-based solution. Thus, a price is set out on privacy [70]. In improving the safety and efficiency of the operation, the economic incentive could adjust to the received data value from the customers by the operator similarly. A framework that explore the interesting direction is not to be conscious.

C. Value-Added Services

By comparing with billing and operations, less attention have been received to the privacy-preserving value-added services. The privacy-preserving demand response is getting much attention in the value-added service [72], [73]. A trusted entity is assumed in the presented scheme in [73] which involves of the submission of bids in the form of power demand by the customers in such a way that they could showing anxiety to the corresponding price and the shed. The secure multi-party computation using secret sharing scheme of Shamir is used by the presented solution in [71] and it depends on a set of schedulers that could be honest-but-curious. Alternatively, an iterative scheme was introduced that includes the assumption of exchanging aggregation consumption plans by the customers with additive noise.

The identification of appliance level anomalies or optimization of electricity consumption of a household could target by the value-added services along with the demand-response and are relevant to the Non-Intrusive Load Monitoring (NILM). Based on the features of energy consumption of a household, value-added services would focus on providing of value to the consumer and metering data requires for various resolutions unlike NILM which has a primary goal of load disaggregation. As services don't require complete time series, the value-added services' feasibility doesn't contradict the operations of privacy-preserving. For an instance, high frequency data may enough for detecting the faulty recrifiers [74]. A characterization of normal behaviour may not available which is an essential aspect of outlier direction. By using unsupervised machine learning, outliers may have to be detected. Example, the distributed algorithms were showed that the detection of privacy-preserving outlier is to be possible with the distance-based methods [75].

For transmission of similar data with different down-sampled versions and protecting each version with a key, the naïve solution would enabled by such value-added services. A hierarchical representation is used as a more sophisticated solution. Example, a wavelet transform is applied recursively on the low pass sub-band [76]. A scheme of hierarchical key management requires in the representations and it ensures that the customer can facilitate a key to the provider of value-added service that facilitates to access the right representations [77]. A source-coding paradigm would be used as an alternative solution as similar as the Multiple Description Coding (MDC) which has been utilized for loss resilient video and audio coding [78]. Various representations with equal importance would be created by an MDC-like scheme and an arbitrary k-subset of these representations could be used by a service provider to encode the data with accuracy for processing the service.

From the persective of resolution definition, researching in this area would get benefitted that the several value-added services require and confirm whether the data is needed continuously

or occasionally. To detect the malfunctioning equipment, a high-pass filtering version of a power consumption of a household may enough but the average consumption of a household wouldn't reveal. For the purpose of data exchange, the infrastructure of public communication is used if high-resolution information require occasionally and may be efficient to use a separate. Low bandwidth would require in the metering infrastructure significantly and the technologies of privacy-preserving are improved for billing and operation. They are not require to extend the high-frequency data for value-added services. Because of the direct connection to the smart meters in the infrastructures of public communication, such solution would rise the cost of data collection infrastructure.

The implementation of value-added services on the private computing platforms of customers would be another alternative, such as the mobile phones. The private data can be kept locally but the delivering of data to the devices can assume as in a privacy-preserving. A number of potential issues are still require to be dealt with. For deploying the algorithms on customer-owned devices, this solution needs value-added service providers primarily and the task of the algorithms to be stolen. Some form of machine learning would employ by many value-added services. Thus, they would be intensive computationally. The comparison of data from different customers would rely by many value-added services which include distributed privacy preserving algorithms to implement the value-added services. To address these problems, the advancements require in the privacy-preserving and energy-efficient distributed machine learning algorithms.

Ref.no	Author name	Proposed work	Importance
43	Alfredo Rial et al., (2011)	While keeping the use of tamper evident meters to a minimum strictly, a privacy-preserving protocol proposes for general calculations on fine-grained meter readings. Based on the readings on own devices, users allow to process and prove the computations' correctness without disclosing any fine grained consumption. By supporting a wide variety of tariff policies, the protocols implement for time-of-use billing as they are simple and efficient.	With the disclosing of fine-grained data consumption to utility providers, the user privacy threaten by the proposals of smart grid. Here, the utility providers include time-of-use billing, energy efficiency advice, tariff, forecasting, settlement, and profiling.
45	Jan CamenischAnna Lysyanskaya (2002)	A scheme of practical and provably secure signature proposes and show protocols (1) to prove the knowledge of a signature on a committed value, and (2) to issue a signature on a committed value (so the signer has no information about the signed value). To design the anonymity-enhancing cryptographic systems, this signature scheme and corresponding protocols are used as building blocks. Here, those systems are group signatures, electronic cash, and anonymous credential	Both as a building block in the design of cryptographic protocol and in its own right, digital signature schemes have been used as a fundamental cryptogrammic primitive.

		systems. Based on the Strong RSA assumption, the signature scheme security and protocols performance is resulted.	
49	Efthymiou; Georgios Kalogridis (2010)	A method demonstrates by the author to anonymize frequent electrical metering data (for example, every few minutes) sent using a smart meter. This information may not require to be attributable necessarily for a specific smart meter or consumer although such frequent metering data may require by an electrical energy distribution network or a utility. However, it needs to be attributable securely to a particular location within the network of electricity distribution like a group of houses or apartments.	It's very essential to maintain the security and privacy of future smart metering networks and smart grid. Eventually, the public accepts to make a research in this area. The of data will require to reassure by smart meter users.
62	Fengjun Li et al., (2011)	An approach of distributed incremental data aggregation presents that process the data aggregation at all involved smart meters in routing the information from the source meter to the collector unit. The entire local neighbourhood or any arbitrary set of designated nodes with minimum overhead covers by the aggregation route based on a constructed aggregation tree carefully. For securing the data enroute, homomorphic encryption is utilized for protecting the user privacy.	While protecting the user privacy, efficient data aggregation supports by this approach in smart grids. This method suits for smart grids that include repetitive routing data aggregation tasks.
60	Rongxing Lu et al., (2012)	An efficient and privacy-preserving aggregation scheme proposes known as EPPA for communications of smart grid. To structure the multidimensional data, a super-increasing sequence uses by EPPA and the structured data encrypts using the technique of homomorphic Paillier cryptosystem. Data aggregation performs on ciphertext directly at local gateways by not including the data communications decryption from user to smart grid operation center, the aggregation result of the original information can	The concept of smart grid has been raised due to the convergence of information and communication technology and traditional power system engineering. It's important to achieve the success of next generation of power grid which featuring efficient, reliable, flexible, secure, friendly, and clean.

		be retrieved. The technique of batch verification adopts by EPPA for reducing the cost of authentication. Different threats of security restricts using EPPA and user privacy preserves which demonstrates through extensive analysis.	
65	Dongwon Seo et al., (2011)	A secure and efficient power management mechanism proposes by author that leverages a homomorphic data aggregation and capabilty-based power distribution. To collect the customers' power demands with security and efficiency and for distributing the power to customers who have the capability, the proposed mechanism is used. The validation of whether the request delivers to the utility properly can perform by each customer and the misbehaving customers who exceed the capabilities can detect by each distributor based on the evaluation.	The smart grid security is the prime consideration of preventing from catastrophic failures as a smart grid gains much attention in a research field due to the features like saving and controlling power generation and consumption. The significant issue is that the excessive power consumption because the power provider can't able to analyse and be responsive promptly for such massive demand that causes blackouts through wide regions.
61	Sushmita Ruj, Amiya Nayak (2013)	A decentralized security framework proposes for smart grids that support access control and data aggregation. By using neighboring area network (NAN), building area network (BAN), and home area network (HAN), data can aggregate in a way that protecting the consumers' privacy. To achieve this, homomorphic encryption technique is used where the collected data of consumers would sent out to the substations which monitor using remote terminal units (RTU). The attribute-based encryption (ABE) uses the proposed access control mechanism that provides access to the stored consumer data selectively in data repositories and is utilized based on different smart grid users. The cryptographic keys and attributes have included in RTUs and users that distributed by various	The scheme of access control is in distributed characteristic and doesn't rely on a single KDC for keys distribution that allows to make the approach as robust one. The primary work is based on the smart grids that integrates the two essential security components such as access control and privacy preserving data aggregation.

		key distribution centers (KDC). Under a set of attributes, encrypted data sends by RTUs.	

2. CONCLUSION

At third-party data centers or utility-managed centers, the smart meter data will manage and process by considering the regulatory framework and business incentives. For computing the confidentiality-preserving data, the fundamental limits for obfuscation-based solutions while considering the model of trusted storage would be investigated. As smart meter data will use the real-time operations, no known solution will be a privacy-preserving public auditing of real-time data that owes the operational safety and financial implications. It's a challenging task to achieve the all requirements of security and privacy in case of preserving the consumer privacy. Based on the studies performed on the value-added services possibility, the progress requires both in the privacy-preserving distributing machine learning algorithms and code protection. To address the issue of privacy economics in a digital environment, both utility theoretic models of privacy [79] and consumer-operator interaction with game theoretic models would be required.

REFERENCE:

[1]. D.-M. Han and J.-H. Lim, "Design and implementation of smart home energy management systems based on ZigBee," IEEE Trans. Consum. Electron., vol. 56, no. 3, pp. 1417–1425, Aug. 2010.

[2]. J. Peppanen, M. J. Reno, M. Thakkar, S. Grijalva, and R. G. Harley, "Leveraging AMI data for distribution system model calibration and situational awareness," IEEE Trans. Smart Grid, vol. 6, no. 4, pp. 2050–2059, Jul. 2015.

[3]. K. Samarakoon, J. Wu, J. Ekanayake, and N. Jenkins, "Use of delayed smart meter measurements for distribution state estimation," in Proc. IEEE PES Gen. Meeting, Detroit, MI, USA, 2011, pp. 1–6.

[4]. P. A. Pegoraro et al., "PMU and smart metering deployment for state estimation in active distribution grids," in Proc. IEEE ENERGYCON, Florence, Italy, 2012, pp. 873–878.

[5]. C. E. Kontokosta, "Energy disclosure, market behavior, and the building data ecosystem," Ann. New York Acad. Sci., vol. 1295, no. 1, pp. 34–43, 2013.

[6]. K. Vatanparvar, Q. Chaun, and M. A. Al Faruque, "Home energy management as a service over networking platforms," in Proc. IEEE PES ISGT, 2015, pp. 1–5.

[7]. S. Karnouskos, "Smart houses in the smart grid and the search for value-added services in the cloud of things era," in Proc. IEEE Int. Conf. Ind. Technol., Cape Town, South Africa, 2013, pp. 2016–2021.

[8]. H. Y. Lam, G. S. K. Fung, and W. K. Lee, "A novel method to construct taxonomy of electrical appliances based on load signatures," IEEE Trans. Consum. Electron., vol. 53, no. 2, pp. 653–660, May 2007.

[9]. N. Batra et al., "NILMTK: An open source toolkit for nonintrusive load monitoring," in Proc. ACM Int. Conf. Future Energy Syst. (e-Energy), Cambridge, U.K., 2014, pp. 265–276.

[10]. Chowdhury, Dhiman, Mehedi Hasan, and Md Ziaur Rahman Khan. "Statistical features extraction from current envelopes for non-intrusive appliance load monitoring." In *2020 SoutheastCon*, pp. 1-5. IEEE, 2020.

[11]. M. Zeifman, "Disaggregation of home energy display data using probabilistic approach," IEEE Trans. Consum. Electron., vol. 58, no. 1, pp. 23–31, Feb. 2012.

[12]. G. Wood and M. Newborough, "Dynamic energy-consumption indicators for domestic appliances: Environment, behaviour and design," Energy Build., vol. 35, no. 8, pp. 821–841, 2003.
[13]. Braun, Trevor, Benjamin CM Fung, Farkhund Iqbal, and Babar Shah. "Security and privacy challenges in smart cities." *Sustainable cities and society* 39 (2018): 499-507.
[14]. M. Jawurek, M. Johns, and F. Kerschbaum, Plug-In Privacy for Smart Metering Billing. Heidelberg, Germany: Springer, 2011, pp. 192–210.
[15]. Friedman and A. Schuster, "Data mining with differential privacy," in Proc. ACM Intl. Conf. Knowl. Disc. Data Min. (KDD), Washington, DC, USA, 2010, pp. 493–502.
[16]. L. Sweeney, "k-anonymity: A model for protecting privacy," Int. J. Uncertainty Fuzziness Knowl. Based Syst., vol. 10, no. 5, pp. 557–570, 2002.
[17]. McLaughlin, Stephen, Dmitry Podkuiko, and Patrick McDaniel. "Energy theft in the advanced metering infrastructure." In International Workshop on Critical Information Infrastructures Security, pp. 176-187. Springer, Berlin, Heidelberg, 2009.
[18]. M. R. Asghar, G. Russello, B. Crispo, and M. Ion, "Supporting complex queries and access policies for multi-user encrypted databases," in Proc. ACM Cloud Comput. Security Workshop (CCSW), Berlin, Germany, 2013, pp. 77–88.
[19]. R. Küsters, E. Scapin, T. Truderung, and J. Graf, Extending and Applying a Framework for the Cryptographic Verification of Java Programs. Heidelberg, Germany: Springer, 2014, pp. 220–239.
[20]. A. Friedman and A. Schuster, "Data mining with differential privacy," in Proc. ACM Intl. Conf. Knowl. Disc. Data Min. (KDD), Washington, DC, USA, 2010, pp. 493–502.
[21]. Wei, Ruoxuan, Hui Tian, and Hong Shen. "Improving k-anonymity based privacy preservation for collaborative filtering." *Computers & Electrical Engineering* 67 (2018): 509-519.
[22]. B.-R. Lin and D. Kifer, "Information measures in statistical privacy and data processing applications," ACM Trans. Knowl. Disc. Data, vol. 9, no. 4, pp. 1–29, Jun. 2015.
[23]. M. R. Asghar and G. Russello, "ACTORS: A goal-driven approach for capturing and managing consent in e-health systems," in Proc. IEEE Int. Symp. Policies Distrib. Syst. Netw. (POLICY), Chapel Hill, NC, USA, Jul. 2012, pp. 61–69.
[24]. J. H. Saltzer and M. D. Schroeder, "The protection of information in computer systems," Proc. IEEE, vol. 63, no. 9, pp. 1278–1308, Sep. 1975.
[25]. R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Rolebased access control models," IEEE Comput., vol. 29, no. 2, pp. 38–47, Feb. 1996.
[26]. Dias, João Pedro, Hugo Sereno Ferreira, and Ângelo Martins. "A blockchain-based scheme for access control in e-health scenarios." In *International Conference on Soft Computing and Pattern Recognition*, pp. 238-247. Springer, Cham, 2018.
[27]. Al-Jawad, Ahmed, Purav Shah, Orhan Gemikonakli, and Ramona Trestian. "Policy-based QoS management framework for software-defined networks." In *2018 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1-6. IEEE, 2018.
[28]. M. R. Asghar, "Privacy preserving enforcement of sensitive policies in outsourced and distributed environments," Ph.D. dissertation, Dept. Inf. Eng. Comput. Sci., Univ. at Trento, Trento, Italy, Dec. 2013. [Online].Available: http://eprints-phd.biblio.unitn.it/1124\.
[29]. Farao, Aristeidis, Christoforos Ntantogian, Cristiana Istrate, George Suciu, and Christos Xenakis. "SealedGRID: Scalable, trustEd, and interoperAble pLatform for sEcureD smart GRID." In *6th International Symposium for ICS & SCADA Cyber Security Research 2019 6*, pp. 74-81. 2019.

[30]. X. Lu, W. Wang, and J. Ma, "Authentication and integrity in the smart grid: An empirical study in substation automation systems," Int. J. Distrib. Sensor Netw., vol. 8, no. 6, Apr. 2012, Art. no. 175262.
[31]. J. Camenisch, S. Hohenberger, M. Kohlweiss, A. Lysyanskaya, and M. Meyerovich, "How to win the clonewars: Efficient periodic n-times anonymous authentication," in Proc. ACM Conf. Comput. Commun. Security (CCS), Alexandria, VA, USA, 2006, pp. 201–210.
[32]. P. P. Tsang, M. H. Au, A. Kapadia, and S. W. Smith, "PEREA: Towards practical TTP-free revocation in anonymous authentication," in Proc. ACM Conf. Comput. Commun. Security (CCS), Alexandria, VA, USA, 2008, pp. 333–344.
[33]. Nizamuddin, Nishara, Haya R. Hasan, and Khaled Salah. "IPFS-blockchain-based authenticity of online publications." In *International Conference on Blockchain*, pp. 199-212. Springer, Cham, 2018.
[34]. H. Pang, A. Jain, K. Ramamritham, and K.-L. Tan, "Verifying completeness of relational query results in data publishing," in Proc. ACM Int. Conf. Manag. (SIGMOD), Baltimore, MD, USA, 2005, pp. 407–418.
[35]. B. Parno, J. Howell, C. Gentry, and M. Raykova, "Pinocchio: Nearly practical verifiable computation," in Proc. IEEE Symp. Security Privacy, Berkeley, CA, USA, 2013, pp. 238–252.
[36]. Yu, Xixun, Zheng Yan, and Rui Zhang. "Verifiable outsourced computation over encrypted data." *Information Sciences* 479 (2019): 372-385.
[37]. M. Backes, D. Fiore, and R. M. Reischuk, "Verifiable delegation of computation on outsourced data," in *Proc. ACM Conf. Comput. Commun. Security (CCS)*, Berlin, Germany, 2013, pp. 863–874
[38]. F. B. de Oliveira, On Privacy-Preserving Protocols for Smart MeteringSystems. Cham, Switzerland: Springer, 2017.
[39]. M. Jawurek, M. Johns, and F. Kerschbaum, Plug-In Privacy for Smart Metering Billing. Heidelberg, Germany: Springer, 2011, pp. 192–210.
[40]. Olalia, Romulo L., Ariel M. Sison, and Ruji P. Medina. "Subset Sum-Based Verifiable Secret Sharing Scheme for Secure Multiparty Computation." In *International Conference on Computing and Information Technology*, pp. 209-219. Springer, Cham, 2018.
[41]. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.
[42]. M. Jawurek, M. Johns, and F. Kerschbaum, Plug-In Privacy for Smart Metering Billing. Heidelberg, Germany: Springer, 2011, pp. 192–210.
[43]. A. Rial and G. Danezis, "Privacy-preserving smart metering," in Proc. ACM Workshop Privacy Electron. Soc. (WPES), Chicago, IL, USA, 2011, pp. 49–60.
[44]. J. Groth, "Non-interactive zero-knowledge arguments for voting," in Proc. Int. Conf. Appl. Cryptography Netw. Security (ACNS), New York, NY, USA, 2005, pp. 467–482.
[45]. J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols," in Proc. Int. Conf. Security Commun. Netw. (SCN), Amalfi, Italy, 2002, pp. 268–289.
[46]. A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in Proc. ACM Workshop Embedded Sens. Syst. Energy Efficiency Build. (BuildSys), Zürich, Switzerland, 2010, pp. 61–66.
[47]. J. Peppanen, M. J. Reno, M. Thakkar, S. Grijalva, and R. G. Harley, "Leveraging AMI data for distribution system model calibration and situational awareness," IEEE Trans. Smart Grid, vol. 6, no. 4, pp. 2050–2059, Jul. 2015.

[48]. K. Samarakoon, J. Wu, J. Ekanayake, and N. Jenkins, "Use of delayed smart meter measurements for distribution state estimation," in Proc. IEEE PES Gen. Meeting, Detroit, MI, USA, 2011, pp. 1–6.

[49]. C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in Proc. IEEE Smart Grid Comm, Gaithersburg,MD, USA, Oct. 2010, pp. 238–243.

[50]. Sultan, Sari. "Privacy-preserving metering in smart grid for billing, operational metering, and incentive-based schemes: A survey." *Computers & Security* 84 (2019): 148-165.

[51]. J.-M. Bohli, C. Sorge, and O. Ugus, "A privacy model for smart metering," in Proc. IEEE Int. Conf. Commun. Workshops (ICCW), Cape Town, South Africa, 2010, pp. 1–5.

[52]. K. B. Frikken, "Secure multiparty computation," in Algorithms and Theory of Computation Handbook, M. J. Atallah and M. Blanton, Eds. Boca Raton, FL, USA: Chapman & Hall, 2010, p. 14.
[Online]. Available: http://dl.acm.org/citation.cfm?id=1882723.1882737

[53]. Gunnala, Sumalatha, and D. S. R. Murthy. "Analysis on Homomorphic Properties of Attribute involved Probabilistic Public Key Cryptosystem based on Sylow P-subgroups." In *2018 3rd International Conference on Communication and Electronics Systems (ICCES)*, pp. 879-882. IEEE, 2018.

[54]. Kumar, Vinod, Rajendra Kumar, Santosh Kumar Pandey, and Mansaf Alam. "Fully homomorphic encryption scheme with probabilistic encryption based on Euler's theorem and application in cloud computing." In *Big Data Analytics*, pp. 605-611. Springer, Singapore, 2018.

[55]. Suwito, Misni Harjo, and Sabyasachi Dutta. "Verifiable E-Voting with Resistance against Physical Forced Abstention Attack." In *2019 International Workshop on Big Data and Information Security (IWBIS)*, pp. 85-90. IEEE, 2019.

[56]. Nagaty, Khaled A. "A public key cryptosystem and signature scheme based on numerical series." *SN Applied Sciences* 2, no. 2 (2020): 1-14.

[57]. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[58]. C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Stanford, CA, USA, 2009.

[59]. B. Vetter, O. Ugus, D. Westhoff, and C. Sorge, "Homomorphic primitives for a privacy-friendly smart metering architecture," in Proc. Int. Conf. Security Cryptography (SECRYPT), 2012, pp. 102–112.

[60]. R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 9, pp. 1621–1631, Sep. 2012.

[61]. S. Ruj and A. Nayak, "A decentralized security framework for data aggregation and access control in smart grids," IEEE Trans. Smart Grid, vol. 4, no. 1, pp. 196–205, Mar. 2013.

[62]. F. Li, B. Luo, and P. Liu, "Secure and privacy-preserving information aggregation for smart grids," Int. J. Security Netw., vol. 6, no. 1, pp. 28–39, 2011.

[63]. F. B. de Oliveira, On Privacy-Preserving Protocols for Smart Metering Systems. Cham, Switzerland: Springer, 2017.

[64]. D. Chaum, "The dining cryptographers' problem: Unconditional sender and recipient untraceability," J. Cryptol., vol. 1, no. 1, pp. 65–75, 1988.

[65]. D. Seo, H. Lee, and A. Perrig, "Secure and efficient capabilitybased power management in the smart grid," in Proc. 9th IEEE Int. Symp. Parallel Distrib. Process. Appl. Workshops (ISPAW), Busan, South Korea, May 2011, pp. 119–126.
[66]. F. Borges, J. Buchmann, and M. Mühlhäuser, "Introducing asymmetric DC-nets," in Proc. IEEE Conf. Commun. Netw. Security (CNS), San Francisco, CA, USA, Oct. 2014, pp. 508–509.
[67]. J.-M. Bohli, C. Sorge, and O. Ugus, "A privacy model for smart metering," in Proc. IEEE Int. Conf. Commun. Workshops (ICCW), Cape Town, South Africa, 2010, pp. 1–5.
[68]. G. Ács and C. Castelluccia, "I have a dream: Differentially private smart metering," in Proc. Inf. Hiding, Prague, Czech Republic, 2011, pp. 118–132,
[69]. H. Sandberg, G. Dán, and R. Thobaben, "Differentially private state estimation in distribution networks with smart meters," in Proc. IEEE Conf. Decis. Control (CDC), Osaka, Japan, Dec. 2015, pp. 4492–4498.
[70]. L. Fan and L. Xiong, "Real-time aggregate monitoring with differential privacy," in Proc. ACM Int. Conf. Inf. Knowl. Manag. (CIKM), 2012, pp. 2169–2173.
[71]. A. Acquisti, C. R. Taylor, and L. Wagman, "The economics of privacy," J. Econ. Literature, vol. 52, no. 2, pp. 405–409, 2016.
[72]. C. Rottondi and G. Verticale, "Privacy-friendly appliance load scheduling in smart grids," in Proc. IEEE SmartGridComm, Vancouver, BC, Canada, Oct. 2013, pp. 420–425.
[73]. C. E. Rottondi, A. Barbato, and G. Verticale, "A privacy-friendly gametheoretic distributed scheduling system for domestic appliances," in Proc. IEEE SmartGridComm, Venice, Italy, Nov. 2014, pp. 860–865.
[74]. A. J. Paverd, A. Martin, and I. Brown, "Privacy-enhanced bi-directional communication in the smart grid using trusted computing," in Proc. IEEE SmartGridComm, Venice, Italy, Nov. 2014, pp. 872–877.
[75]. R. Isermann, Fault-Diagnosis Applications: Model-Based Condition Monitoring. Heidelberg, Germany: Springer-Verlag, 2011.
[76]. J. Vaidya and C. Clifton, "Privacy-preserving outlier detection," in Proc. IEEE ICDM, Brighton, U.K., 2004, pp. 233–240.
[77]. D. Engel, "Wavelet-based load profile representation for smart meter privacy," in Proc. IEEE PES Innov. Smart Grid Technol. (ISGT), Washington, DC, USA, Feb. 2013, pp. 1–6.
[78]. C. D. Peer, D. Engel, and S. B. Wicker, "Hierarchical key management for multi-resolution load data representation," in Proc. IEEE SmartGridComm, Venice, Italy, Nov. 2014, pp. 926–932.
[79]. V. K. Goyal, "Multiple description coding: Compression meets the network," IEEE Signal Process. Mag., vol. 18, no. 5, pp. 74–93, Sep. 2001.
[80]. A. Acquisti, L. K. John, and G. Loewenstein, "What is privacy worth?" J. Legal Stud., vol. 42, no. 2, pp. 249–274, Jun. 2013.