Architecture and Data Flow Model for Consumer-Oriented Smart Meter Design

Rani Yesudas rani.yesudas@anu.edu.au
College of Engineering and Computer Science,
The Australian National University,
Canberra, Australia.

Roger Clarke roger.clarke@anu.edu.au
College of Engineering and Computer Science,
The Australian National University,
Canberra, Australia.

Abstract

The power grid needs modernisation to efficiently manage the needs of the ever growing population. Smart metering systems have been the main area of focus in smart grid. Smart meter rollouts have started in many countries, but the majority of them are facing resistance from end-users, particularly residential consumers. Generally, consumers have the scheme imposed on them, they are required to pay for the new device, they have little control over their power usage, and they have no control over the considerable amount of additional personal data that the device collects. In this article we identify means of reducing consumer concerns about the data that is extracted and transmitted. We in particular, propose a Smart Metering System Architecture with controls and choices for the consumer, and an abstract data flow model that identifies the security and privacy requirement at each point in the flow.
Keywords: Smart Meter, Advanced Metering Infrastructure (AMI), Data Flow Model, Smart Metering Architecture, Consumer Concern, Technology Acceptance.

1. Introduction

The traditional power-grid is no longer adequate to cope with increasingly extensive and intensive use of electrical devices, and the generation of power within what was previously a transmission and distribution network. Modernisation of the grid is necessary, through the integration of intelligent sensors, controls, robust communications and other technologies. Of all the components in the smart grid, smart meters have attracted the most attention [9, 10]. The majority of grid modernisation projects appears to be focusing their investment on smart meters and advanced metering infrastructure (AMI).

Smart meters enable the recording of power consumption at short intervals, and access to that data by at least the utility and perhaps other organisations in the supply chain. This provides a basis for the imposition of a time-of-use (TOU) tariff. The idea was projected that this would help in reducing the consumption of electricity during peak periods, and thereby enable the postponement of the construction of new power plants, perhaps even indefinitely [9,10]. This would result in savings in capital expenditure and associated borrowing costs, and contribute to reductions in carbon emissions. Smart meters were also claimed to be an enabler of such smart grid features as real-time power-outage tracking and management of power-exportation from renewable sources such as solar panels [8, 9, 10]. These functionalities offer benefits and possibilities to various stakeholders in the grid. Proponents of these projects expected consumers to accept smart meters as a device that would enable them to manage their own power usage. The assumption was made that, by making consumer usage available to them in real-time, together with information about the cost of that usage, particularly during peak periods, they would change their energy usage patterns [8, 9, 10]. It is unclear to what extent those propositions were evidence-based, and to what extent they were merely aspirations.

In practice, smart meter projects have faced considerable resistance from consumers [1, 2]. This strongly suggests that project sponsors failed to understand consumers' needs and concerns, and/or failed to communicate the advantages, and/or failed to have suitable answers to the criticisms levelled at the schemes. Consumers view smart meters with distrust. They perceive smart meters to be a means whereby utilities can maximise their benefits at the expense of consumers' costs, choice, privacy, and even health.

For expensive infrastructure like an economy-wide smart meter system, it is important to achieve consumer confidence. Particularly in the face of activism over issues like security, privacy and health effects, a project-sponsor may spend years battling to convince consumers of the benefits of smart meters [1, 2, 16]. Unless a technology is equipped to act as a support to end-user, it will not be welcome even if it could contribute to solving major issues like lowering carbon emissions and climate change.

The purpose of the research reported in this paper was to address the needs of project sponsors, by showing how consumer resistance to smart meters can be overcome, but to do so in such a manner that consumers' needs are actually addressed. The means whereby this is achieved is by outlining a consumer-friendly design. Key characteristics of such a design include firstly recognition of consumer concerns and of the variability of those concerns across various consumer segments, secondly features that directly address those concerns and are seen by consumers to do so, but also technical feasibility, and compatibility with existing technologies.

The research method adopted was as follows:

1. We identified ways to reduce consumer concern about the data that is collected and accessed by organisations.
2. We undertook a consumer segmentation study, based on subjective control over smart meters.
3. We proposed a Smart Metering System Architecture with controls and choices for the consumer.
4. We prepared an abstract Data Flow Model that identifies the security and privacy requirement at each point in the flow.

The work's contribution is to build on the limited prior literature on the specific question of consumer-oriented smart-meter design, and establish a basis for evaluating existing products and devising new products that better meet the needs of consumers and scheme sponsors alike.

2. Consumer Concerns

In many places, smart meter rollouts have been delayed and even stopped. Even mandated schemes have been halted due to the strong involvement of consumer advocacy groups [1, 2]. If customers' first experiences with smart meters are negative, their trust in the smart meter system will be low. And if trust is low, then it will be challenging to motivate customers to use them, and to participate in demand response in the future.

There are significant unresolved consumer concerns about smart meters [1, 2, 6, 16]. Some consumer concerns may be perceptions rather than actual risks. For example, many communications devices generate electric and magnetic fields (EMF), smart meters generate less traffic than many other such devices, and the nature and extent of EMF-related health risks are in any case contentious matters.

A further issue has arisen from the impression conveyed by many proposals that demand response functionality will provide the utility with the capability to unilaterally shut down the consumer's appliances in order to reduce load. This would represent a substantial limitation on consumers' rights to self-determination. This is commonly referred to as a 'choice' issue.

Many media reports depict the smart meter as a spy in the home. Research evidence shows that smart meter data at one-minute intervals are capable of providing insights into a household's appliances and activities, thereby revealing the residents' living patterns [15]. On the other hand, measurements of lower granularity would appear to make it more difficult to infer such information.

From the consumer's viewpoint, smart meter schemes appear to be demanding that they pay for a new meter, learn new skills, use them frequently, change their usage patterns of their appliances, give up some control over their appliances, and even permit the escape of potentially sensitive personal data. It is unsurprising that consumers are inclined to believe that the real purpose of smart meters is to enable energy suppliers to increase their profits at consumers' expense.

All of these concerns are real, irrespective of the extent to which they are justifiable. They represent impediments to the adoption of smart meters, and barriers to both return on investment and the ultimate objectives of efficient power-production and –delivery, and lower environmental impact.

The focus in the remainder of this article is on privacy and choice issues. A theoretical basis is provided by recognition that negative emotions arise from a subjective loss of control, and that negative emotions greatly reduce a person's preparedness to use a technology [3]. Kranz et al. conducted research to explore the role of control on the acceptance of smart meters [12]. They extended the Technology Acceptance Model (TAM) by adding subjective control as a construct. A survey of 351 participants found that subjective control was the second-strongest element behind perceived usefulness, and a major determinant of the intention to use smart meters [12].

A summary of existing literature revealed that few articles reflect much depth of appreciation of consumer concerns and what can be done about them. McKenna et al. [14] examined how to minimize data requirements for the main functionalities of smart meter data in order to reduce consumer concerns. However, the method that they propose fails to offer options suitable for different consumer segments. Kranz et al. [13] diagrammatically represented information flow of data to and from smart meter, but did not examine ways to reduce consumer concerns. Berthier et al. [5] listed possible threats targeting an AMI and suggested an architecture that addresses one specific aspect – monitoring and intrusion detection. Their proposal did not, however, identify all of the points of vulnerability in such systems.

Chinnow et al. [7] analysed security and attack scenarios of smart metering architecture and protocols as used in Germany. However, they did not focus on consumer needs, controls and options. Gungor et al. [10] presented an AMI architecture, but again pays very little attention to consumer needs. Wang et al. [17] discussed the communication architecture of the grid as a whole, including smart meters. Berihun & Alavoine [4] represented a 'prosumers' house using a smart meter, and identified possible attacks and threats. However, unlike our own work conducted in parallel with theirs [18], their analysis missed many points of vulnerability because they failed to drill down to sufficient depth.

The remainder of this paper identifies consumer segments, reflects the varying priorities of different categories of consumers, and presents an architecture, design features and a data flow analysis that address the key issues that represent impediments to adoption.

3. Means of Addressing Consumer Concerns

On the basis of the analysis in the preceding sections, we propose a set of constructive measures that address consumer concerns about choice and privacy, and that thereby increase consumer confidence on the system. Four aspects are outlined: categories of data, consumer segmentation, architecture and data flow.

3.1. Categories of smart meter data

Smart metering data can be usefully classified into three categories: (i) Billing operations data; (ii) Demand Response data; and (iii) Grid intelligence data. The third category involves alerts about power-outages and Quality of Service (QoS). Such data is limited in its sensitivity, and disclosures occur very infrequently and with direct benefits to the consumer.

The primary focus of privacy and choice concerns are the other two categories. Table 1 provides a discussion of the nature and purpose of categories i) and ii), and design features that address consumer concerns.

3.2. Consumer Segmentation based on their concerns about smart meters

Consumers' reactions to smart meters vary from extreme resistance to high acceptance. There are consumers who see a smart meter as a device that causes serious health effects and there are also technology enthusiasts who would like to use every possible feature provided by it to manage their power consumption. Some people don't mind detailed meter reading but don't want the smart meter to manipulate or control their appliances. Based on this we have identified 5 smart meter consumer segments as shown in Table 2.

Table 1. Options to reduce consumer concern over Smart Meter data

	Billing Operation	**Demand Response operation**
Purpose	Electricity is a service that needs to be paid for and hence the utility provider needs details of consumption to charge the consumer.	This data is required for identifying the rise and fall in demand in a locality.
Data Frequency	i) Less frequent and cyclic ii) Intervals: Monthly / Quarterly / etc.	i) More Frequent ii) Intervals : 15 mins/ 30 mins / 1 hr /etc.
Effects on Consumer	Because of the low level of granularity, this data represents a very limited privacy threat, and has long been accepted as being a necessary element of the service.	This data is required frequently with or without a request. The transmission frequency can be programmed in the meter and back-end. This data could breach the security and privacy of the consumer.
Data Requirement	As this data has no other purpose apart from billing, it is only required on request from utility. Utility can send a request to fetch the billing data as per the billing cycle chosen.	Demand response data can be sent at intervals that are programmed at the meter or when triggered by requests sent from utility.
Options to reduce consumer concern		
Permission Control	i) Consumers exhibit limited concern about permission controls for this data. Billing data is the only method by which the consumption can be calculated and hence needs to be performed without any hindrance. ii) Consumers can be given the choice of billing intervals with a limit of one setting per cycle.	i) Consumer should be provided with choices on frequency of data storage, transmission and permissions to modify the energy usage. ii) There should also be options to disable transmission permanently or temporarily.
Storage settings	The data stored should be read-only. The data should be protected from unauthorized deletion and modification. This data should be available for billing verification in case of disputes	The data stored should be read-only. The data should be protected from unauthorized deletion and modification. This data should be available to other organisations only under strict controls. In particular, access for law enforcement purposes requires reasonable grounds for suspicion of relevance to the investigation of a criminal offence, and demonstrated legal authority.
Transmission settings	Billing should be calculated in the meter based on the TOU tariff declared. This eliminates the need to send detailed data for billing purpose. The data that required can be reduced to : a) Final (Present) Meter Reading b) Details of consumption accumulated under each period e.g. peak, off-peak and shoulder. This can be used to verify the bill calculation. c) Bill amount.	End user details are not required for grid operations, hence this data transmitted should be anonymous (when data leaves the smart meter) and aggregated at the data concentrator (this should be a point in the system close to the consumer and remote from the utility) to protect the privacy of the consumer.

Table 2. Consumer Segments based on their reaction to Smart Meter

	User Characteristics	**User Reaction**
Type 1	They strongly object to the escape of personal data from their premises.	High resistance
Type 2	They don't mind having a communicating device installed but don't trust the meter functionality and they don't want any support and prefer to manage energy personally.	Low resistance
Type 3	They don't mind having a smart meter, but they want a very basic setting programmed into it, and do not want to make changes, preferably ever.	Neutral

Type 4	They would like to receive alerts and information through a smart meter but would personally make the changes.	Low acceptance
Type 5	Technology enthusiast and energy conscious user. They want to take maximum advantage of the functionalities provided, including programming the meter to switch particular appliances off during peak periods.	High acceptance

3.3. Consumer Oriented Smart Metering Architecture

A smart metering system mainly consists of a smart meter, a collector/ concentrator, communication network and a head-end data storage system [11]. An in–house-display (IHD) module is an optional device that helps the consumer monitor their energy usage in real-time. The smart meter consists of the metering module and a communication module with the network interface card (NIC). Some smart meters have a detachable communication module that can be easily plugged into the main module. This provides the advantage of using the metering module even if the communication technology is changed. The communication network ideally requires a comprehensive set of security safeguards which may not be present in current advanced metering infrastructure (AMI) systems. There are also online energy management systems but they are not yet advanced to the stage where consumer can modify their energy profile and meter settings. Currently using the online portal, consumers can check their power consumption, meter profile and receive alerts and message from the utility provider [19].

The proposed architecture of consumer oriented smart metering system is shown in Fig. 1and Table 3 presents controls and choices that can be provided to different users through this architecture. The critical differences are that consumer has the choice to remove the communication module and consumer also has control over both the data recording intervals and the intensity and frequency of data transmission. These specific features provide consumer with control and choice reducing the intensity of data available to the utility thereby achieving consumer acceptance.

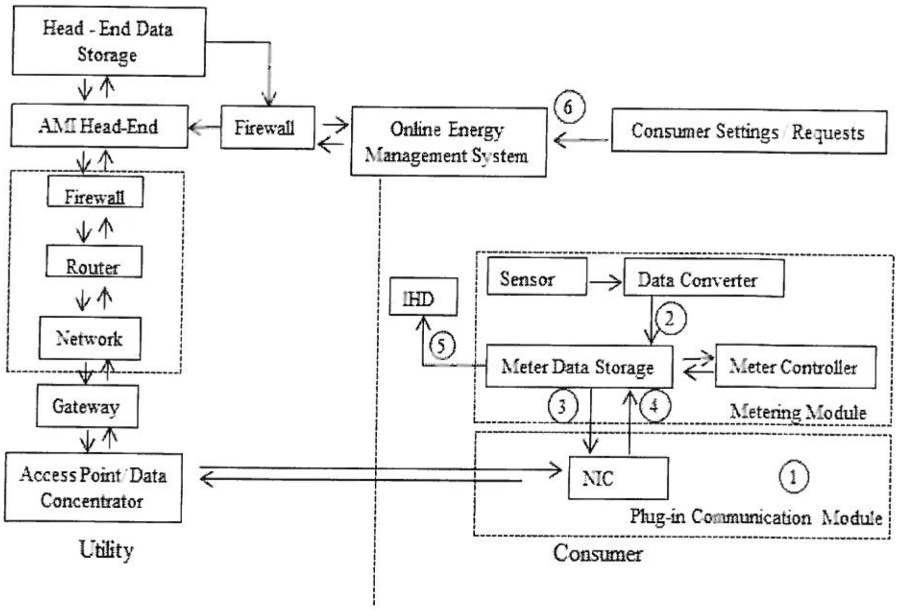

Fig. 1. Consumer Oriented Smart Metering System Architecture

Table 3. Controls/Choices in the smart metering system architecture for different user types

Option	User Type	Remarks
1. Plug –in Comms module	Type 1	1. If the communication module is of plug-in type, it can be removed for consumers that don't want a radiating device in their premises. Such meters have to be manually read and the utility may have to charge those consumers extra for labour cost. In future if they wish to use the data transmission functionality the communication module can be easily plugged in. 2. As there is no data transmitted to the head- end, details like outage and issues in QoS have to be communicated manually by the consumer. 3. Limitations - Consumers who worry about RF emission health issues may still be affected by radiations from neighbouring consumer's meter or collectors in the locality.
2. Choice in the interval of LP data storage	Type 1	As Type 1 user will not have a communication module, there is no requirement for them to store load profile data. Hence for such consumers there should be options to disable load profile channels and record no data. There could also be options for larger interval if required (e.g. 15 days / 1 month)
	Type 2	As Type 2 user will personally manage their energy consumption, they won't require frequent interval data. There should be option to program such users to larger intervals with just enough to supply information for grid operations.
	Type 3 Type 4 Type 5	These users favour frequent data collection and hence there should be 2or 3 options in the choices of shorter intervals (10 min /15 mins/30 mins)
3. Frequency and interval of data transmission	Type 2 Type 3 Type 4	There should be options to : 1. Choose the interval of data transmission. It can be different from the interval in which data is stored. 2. Disable data transmission permanently or temporarily. Though the data can be anonymised and later aggregated during transmission there should be choice provided to disable data transmission. This will ease the worries of the consumer who think their energy consumption data could be used to profile them and distinguish if their premises are occupied or not. 3. Modifications to the data transmission should be notified to the head-end, so that they can use prior knowledge or other intelligence to calculate demand response. 4. Alerts like power outage and variations to QOS from the set thresholds don't affect consumer choices and hence that information should be transmitted to the back end without any interference.
4. Meter actions/ alerts/ Energy usage variations	Type 2	These users prefer not to use any help for their energy management, they only require options to receive alerts. Those alerts can be made available through In-House-Display or Online Energy Management system.
	Type 3	These users prefer not to constantly change their settings. Such consumers can be given the option to have the smart meter modify their energy usage during peak period declaration. If they have equipments with high energy requirement, that are not urgent they could be connected to the LC relay and made to switch off or cycle as per need.
	Type 4	These users prefer to be provided with alerts but wants the freedom to make choice of their energy usage.
5. Displaying usage with IHD	Type 1 Type 2 Type 3 Type 4 Type 5	All users, including the Type 1 user can utilise an IHD display to monitor consumption and other metering data at real-time, but Type 1 users won't be able to display alerts from the utility as they don't have a communication module. The smart meter should have a customisable display list for data to appear in IHD and there should be options to program the meter display based on consumer preference.
6. Setting Profile using online management	Type 4	As these users would prefer to make changes personally, they can be given option through Online Energy Management system to make changes to the LC relay settings. Any equipment that is connected to the LC relay will then perform as per their chosen settings.

system	Type 5	Technology enthusiast and energy conscious user who would like to make frequent changes to their profile settings can be provided with advanced options in online management systems for submitting their requirements. These requests should be first send to the Head-End and upon approval applied to the smart meter profile.

3.4. Abstract Data Flow Model

The architectural features outlined in the previous section create potentials, but do not in themselves deliver the features. In this section we identify security and privacy requirements at each point of flow of meter data. In Table 4, we have classified data stored in the meter into six categories based on their functionalities. Fig. 2 presents an abstract data flow model for smart meter data. In Table 5, we have listed the security and privacy requirements at each point of the flow which addresses the key consumer concerns.

Table 4. Categories of data stored in the Smart Meter

Meter Data Type	Data Functionality
Detailed Data	This includes load profile data that is recorded at frequent intervals .This information is used for demand response and related operations
Accumulated Data	This includes accumulated consumption data which is not required frequently and in most cases, needs to be only sent when requested by utility. E.g. Billing operations.
Meter Profile Data	This data contains settings that determine how the meter operates. Most smart meters have a load control (LC) relay and they can be made to operate differently from the main load by settings in the meter profile. Settings can also be provided to override operations commands from the utility.
Command Data	This data includes command and control operations received from utility. This data along with meter profile setting controls meter operations.
Display Data	This includes data that be programmed to be displayed in the meter's display unit and in other devices like IHD.

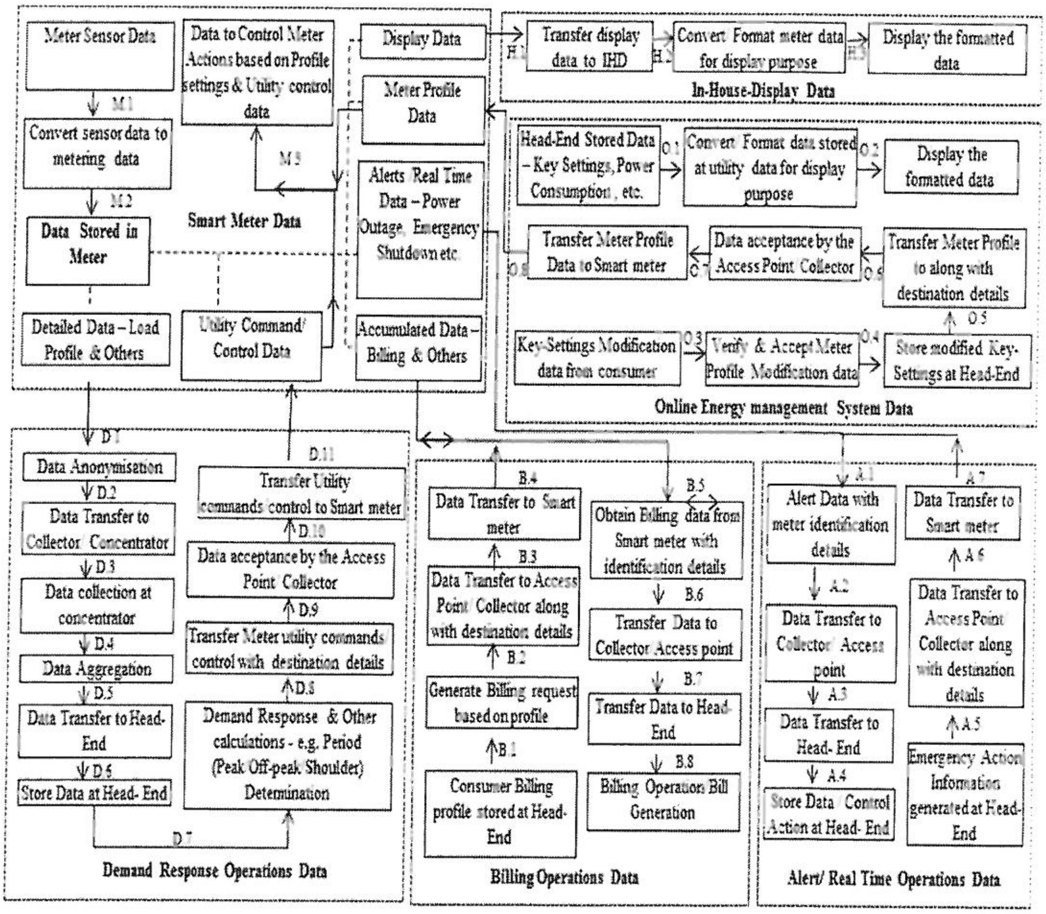

Fig. 2. Abstract Data Flow Model for Smart Metering System

Table 5. Security and Privacy requirements for Meter Data at each point of flow

	Security and Privacy requirement	
General requirement		
G.1	There should be measures to ensure accuracy in data conversions and calculations. The integrity and authenticity of the data should be assured.	
G.2	During data transfer, there should be measures to prevent loss and corruption. There should be measures to prevent interception and tampering. The integrity, authenticity and confidentiality of the data should be assured.	
G.3	At various stages metering data will require formatting. Correct profiles and settings have to be chosen for each formatting to provide meaningful information. The integrity and utility of data should be assured.	
G.4	During data storage there should be measures to prevent loss and corruption. There should be measures to ensure the storage is tamper proof. The integrity, authenticity, confidentiality utility of data should be assured.	
Point		**Apply**
Smart Meter Data		
M.1	Readings from the meter sensors are converted to metering data.	G.1
M.2	The converted sensor data is stored in meter.	G.3 G.4
M.3	Data to control meter operations (e.g. cycling the load, service disconnect etc.) are derived from meter profile setting and commands obtained from the head-end. There should be measures to ensure that the control information is accurately derived based on the priorities set in meter profile. This data is very critical as it has the capability to modify meter operations and even cause disruption of service.	G.1
	Demand Response Operations Data	
D.1	For demand response, the identification details of the consumer operations are not essential. To ensure privacy the data should be anonymised. This will reduce consumer concerns of being profiled from frequently communicated data from the meter.	G.1
D.2	The retrieved data is transferred from meter to collector. The data may undergo formatting before transfer.	G.2 G.3
D.3	The linked collector should receive the data after verification.	G.2
D.4	Data aggregation should be done to the demand response data received from multiple end-points linked to a collector. This will further secure the system from privacy threats as the data that is transferred further up the system will be linked to the collector and not a particular individual.	G.1
D.5	The aggregated data should then be transferred to the head-end.	G.2 G.3
D.6	The received data should be accepted and stored at head-end. The data may require conversion to the format suitable for storage.	G.3 G.4
D.7	Based on the interval data, the demand response and related calculations should be made and control operations (TOU determination, breaker and LC relay operations, planned outages) need to be determined.	G.1
D.8	Operation information from utility needs to be transferred along with destination details. As one provider may have many linked collectors, it is essential that control data is matched with the exact collector.	G.3
D.9	The control commands could be broadcasted or sent specifically to the collector. In either case the collector should verify the destination details and accept the data.	G.2 G.1
D.10	The received control commands are sent to all meters linked to the collector.	G.2 G.3
D.11	As data sent to head-end is anonymised and aggregated, the demand response operations will be for all meters linked to the collector. The command operations received from the collector gets stored as utility operations data and after verifying with meter profile data, the meter control actions will be generated.	G.4 G.3 G.1
Billing Operations Data		
B.1	The consumer billing profile data should trigger a billing request based on settings.	G.1
B.2	Billing request generated at utility needs to be transferred along with meter identification details. The meter identification details must be able to locate the linked collector.	G.2 G.3
B.3	As there are meter identification details, the billing requests need to be only transferred from collector to the specific meter.	G.2 G.3
B.4	On reception of billing request, the meter should trigger functionality to retrieve billing data.	G.1
B.5	The fetch process should extract the necessary information from the stored accumulated data.	G.1 G.3
B.6	The retrieved data may be formatted and then transferred from meter to collector.	G.3 G.2
B.7	Data received from the collector is transferred the head-end.	G.2

B.8	The billing data needs to be stored at the head-end. The data may require further conversion to the format suitable for storage. Using the received data, billing statement needs to be issued to the consumer.	G.3 G.4 G.1
Alert/ Real-Time Operations Data		
A.1	The meter has standard set of events that trigger alerts and other events can also be programmed to create an alert. Standard events include power outage and programmable events include variation in QoS where the thresholds are set by the consumer or provider. When such events are triggered, the meter should trigger functionality to immediately generate alert.	G.1
A.2	The retrieved data may be formatted and then transferred from meter to collector.	G.3 G.2
A.3	Data received from collector is transferred head-end.	G.2
A.4	The alert data should either trigger correction measures automatically or notify the utility provider to take necessary actions. This data should also be stored at the head-end and may require formatting before storage.	G.1, G.3 G.4
A.5	If there are critical situations at the head-end, such information should also be informed to the consumer in the form of alerts, so that consumer can be prepared for the situation. For e.g. if there is planned outage, it should be communicated to the consumer in real-time. Such events should immediately generate alerts and this information from utility needs to be transferred along with destination details.	G.1 G.3
A.6	The information from head-end could be broadcasted or sent specifically to the collector. In either case, the collector should verify the destination details and accept the alert data.	G.2 G.1
A.7	The data from the collector could be sent to a specific meter or to all linked meters. In either case, the meter should verify the destination details and should only accept the alert data if the credentials match.	G.2 G.1
In-House-Display Data		
H.1	The meter will have a list of items that can be chosen to be displayed. The usual display items includes, instantaneous and cumulative consumption, import energy, export energy, alert data etc. These can be programmed to the meter profile's display settings. The data for items chosen should be extracted from the stored meter data.	G.1
H.2	Display data is transferred from meter to IHD.	G.3 G.2
H.3	As IHD is meant to enhance consumer understanding of energy usage and choices, the raw data from meter needs to be processed to be informative. There should be options in IHD to set thresholds for relevant display items, so that it could alert the consumer if the thresholds are breached.	G.1 G.3
Online Energy Management System Data		
O.1	Through online energy management systems, any end-user related data that is stored at head-end can be made available to the respective consumer. This system should provide user the opportunity to verify meter data in their premises and that stored at the back-end. The information available through this system can easily profile or identify a consumer; hence like any other online management system, this system should be highly secure.	G.4
O.2	The raw data stored in Head-End from meter needs to be processed to be informative. The data conversion and other functions provided should be accurate and tamper proof.	G.1 G.3
O.3	There should be secure option to modify meter profile settings and only the key settings should be transferred to the Head-End. The head-end should be able to accurately verify the source before accepting the data.	G.2 G.1
O.4	The received data should modify the profile settings stored at the head-end. The data may require conversion to the format suitable for storage.	G.1 G.3 G.4
O.5	After storage at Head-End, the modified meter profile needs to be transferred to collector along with meter identification details.	G.3 G.2
O.6	The collector should be able to verify the meter credentials and accept the profile data of a linked meter.	G.1
O.7	As there are meter identification details, the profile data need to be only transferred from collector to the specific meter.	G.2 G.3
O.8	The meter should verify the destination details and if matched, should accept the modified the meter profile.	G.1 G.4

4. Conclusions and Implications

Smart metering projects are at risk of consumer rejection, and investment failure. Research has identified that subjective loss of control can lead to negative consumer emotions resulting in a lower likelihood of acceptance of a smart meter. This paper has identified ways in which consumers' privacy and choice concerns about data that is extracted and transmitted from a smart meter could be reduced. It has also proposed a Smart Metering System Architecture and abstract data flow model that identifies security and privacy requirements to ensure consumer control and choice. This addresses the key requirements identified at the beginning of the paper. It builds on prior work by adopting a consumer perspective on data aggregation and anonymisation, and providing a framework, and checklists of features that need to be delivered by the meter manufacturers.

New projects can adopt the conceptual design presented above. This will enable technical analysis and field-piloting, both of which are essential further steps in validating the proposition. In addition, the architecture and data flow model provide a basis for evaluating existing products, enabling projects to adapt their designs towards this model. This will reduce project risk, increase adoption, improve return on investment, and even salvage some projects from impending disaster.

We intend extending this work, in order to identify the best security measures that would be feasible for different contexts such as geographical location, density of population and the communication technology used.

References

1. ABC News: Smart meters could be abandoned. In: Australian Broadcasting Corporation Online News, (2010).
2. Bayar, T.: Will Germany Reject Smart Meters?. In: Renewable Energy World, (2013)
3. Beier, G., Spiekermann, S., and Rothensee, M.: Die Akzeptanz zukünftiger Ubiquitous Computing Anwendungen. In: Mensch und Computer im Strukturwandel, A. Heineke and H. Paul (eds.), pp. 145-154, Oldenbourg, Munich (2006).
4. Berihun, N. G., Alavoine, F.: Smart Metering Scenario CORAS Method. (2013).
5. Berthier, R., Sanders, W. H., Khurana, H.: Intrusion detection for advanced metering infrastructures: Requirements and architectural directions. In: First IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 350-355, (2010).
6. Betz, J.: 'Smart' Meters Under Fire as Electric Bills Soar. In: Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11. In: WFAA, (2010).
7. Chinnow, J., Tonn, J., Bsufka, K., Konnerth, T., Albayrak, S.: A tool set for the evaluation of security and reliability in smart grids. In: Smart Grid Security, pp. 45-57, Springer Berlin Heidelberg (2013).
8. Fan, Z., Kulkarni, P., Gormus, S., Efthymiou, C., Kalogridis, G., Sooriyabandara,M., Chin, W. H.: Smart grid communications: Overview of research challenges, solutions, and standardization activities. In: Communications Surveys & Tutorials, IEEE, 15(1), pp.21-38, (2013).
9. Fang, X., Misra, S., Xue, G., & Yang, D.: Smart grid—the new and improved power grid: a survey. In: Communications Surveys & Tutorials, IEEE, 14(4), pp.944-980 (2012).
10. Gungor, V.C., Sahin, D., Kocak, T.,Ergut, S., Buccella, C., Cecati, C., Hancke, G.P.: A Survey on Smart Grid Potential Applications and Communication Requirements. In: Industrial Informatics, IEEE Transactions, vol.9, no.1, pp.28,42, (2013).
11. Karnouskos, S., Terzidis, O., Karnouskos, P.: An advanced metering infrastructure for future energy networks. In: New Technologies, Mobility and Security, pp. 597-606, Springer Netherlands (2007).
12. Kranz, J., Gallenkamp, J. V., Picot, A.: Exploring the Role of Control-Smart Meter Acceptance of Residential Consumers. In: Proceedings of the Sixteenth Americas Conference on Information Systems, pp.315. Peru (2010).
13. Kranz, J., Gallenkamp, J., Picot, A.: Power Control to the People? private consumers' acceptance of smart meters. (2010).

14. McKenna, E., Richardson, I., Thomson, M.: Smart meter data: Balancing consumer privacy concerns with legitimate applications. In: Energy Policy, 41, pp. 807-814, (2012).
15. Quinn, E. L.: Privacy and the new energy infrastructure. In: SSRN eLibrary, (2009).
16. Špindlerův, M.: How Smart metering pilot project lost illusions and ideas or nothing is just BLACK and WHITE!. Enel, (2012).
17. Wang, W., Xu, Y., Khanna, M.: A survey on the communication architectures in smart grid. In: Computer Networks, 55(15), pp. 3604-3629, (2011).
18. Yesudas, R., Clarke, R..: A Framework for Risk Analysis in Smart Grid - Perspective Based Approach. In: Proc. 8th Int'l Conf. on Critical Information Infrastructures Security (CRITIS), Springer International Publishing, pp. 84-95, Amsterdam (2013).
19. Zafar, N., Arnautovic, E., Diabat, A., Svetinovic, D.: System security requirements analysis: A smart grid case study. In: Systems Engineering, 17(1), pp.77-88, (2014).