

Discover Internet of Things

Research

Uncertainty propagation in the internet of things

Shantanu Pal¹ · Sara Khalifa² · Dimity Miller³ · Volkan Dedeoglu⁴ · Ali Dorri⁵ · Gowri Ramachandran² ·
Peyman Moghadam⁶ · Brano Kusy⁴ · Raja Jurdak⁵

Received: 15 June 2024 / Accepted: 25 November 2024

Published online: 19 December 2024

© The Author(s) 2024 OPEN

Abstract

The Internet of Things (IoT) detects context through sensors capturing data from dynamic physical environments, in order to inform automation decisions within cyber physical systems (CPS). Diverse types of uncertainty in the IoT pipeline can propagate within and across nodes, involving complex interactions with security, privacy, and trust that remain largely unexplored. This paper conducts an in-depth analysis of the types of uncertainties in IoT and how they propagate within IoT nodes and networks. We consider adversarial uncertainty in the context of distributed IoT networks to capture perturbations due to malicious actors in the network that can influence IoT security, privacy and trust. We examine the propagation of adversarial uncertainty and well-known uncertainty types, namely aleatoric and epistemic uncertainty, within the five distinct stages of sensing, communication, storage, processing and decision-making in an IoT pipeline, across network layer boundaries, and across nodes within an IoT network. Using this mapping, we analyse the interactions between the uncertainty types and their propagation, and security, privacy, and trust in IoT. Based on this analysis, we discuss guidelines and considerations for mitigating uncertainty in IoT through a smart grid use case study.

Article highlights

- We map interactions between uncertainty types (aleatoric, epistemic, adversarial) and IoT security, privacy, and trust.
- We analyze uncertainty sources in IoT, focusing on adversarial impacts in distributed IoT networks.
- Guidelines are derived to mitigate IoT uncertainties using emerging solutions.

Keywords Uncertainty · Internet of things · Data · Security · Privacy · Trust

✉ Shantanu Pal, shantanu.pal@deakin.edu.au; Sara Khalifa, sara.khalifa@qut.edu.au; Dimity Miller, d24.miller@qut.edu.au; Volkan Dedeoglu, volkan.dedeoglu@csiro.au; Ali Dorri, ali.dorri@qut.edu.au; Gowri Ramachandran, g.ramachandran@qut.edu.au; Peyman Moghadam, peyman.moghadam@csiro.au; Brano Kusy, brano.kusy@csiro.au; Raja Jurdak, r.jurdak@qut.edu.au | ¹The School of Information Technology, Faculty of Science, Engineering and Built Environment, Deakin University, Melbourne VIC 3125, Australia. ²The School of Information Systems, Faculty of Science, Queensland University of Technology, Brisbane, QLD 4000, Australia. ³The School of Electrical Engineering and Robotics, Faculty of Engineering, Queensland University of Technology, Brisbane, QLD 4000, Australia. ⁴The Distributed Sensing Systems Group, Data61, CSIRO, Pullenvale QLD 4069, Australia. ⁵The School of Computer Science, Faculty of Science, Queensland University of Technology, Brisbane QLD 4000, Australia. ⁶The CSIRO Robotics, Data61, CSIRO, Pullenvale QLD 4069, Australia.



1 Introduction

With the rapid development of smart sensing technology, portable, low-cost embedded and embodied wireless devices within the Internet of Things (IoT), it is predicted that there will be 50 billion Internet-connected devices by the year 2025 [1]. IoT sensors are deployed in physical environments to dynamically capture local context, process or share this information, and drive decisions that can include actuation to affect the environment. IoT networks are underpinning automation in many industries, and are being increasingly coupled with advanced data analytics and Machine Learning (ML). As these systems are embedded into physical environments, they are subject to the presence of uncertainty [2]. Uncertainty can be seen as a parameter that determines the quality and usefulness of information a system provides. It can stem from different parts of a system, e.g., measurements from sensor data, devices malfunctioning, or lack of knowledge in ML models. In other words, uncertainty may arise from the node behavior, particularly when malicious nodes are part of the network, or from partial or incomplete observations from physical and digital data. Such uncertainties can propagate through the network, lead to unreliable data and predictions, and more importantly drive sub-optimal automation decisions, with the potential for severe consequences.

The uncertainty can also affect the security, privacy, and trust in a standard IoT system which are essential to protect from unauthorised access and ensure performance reliability. Security is typically a mechanism protecting a system and information from abuse, fraud, and unauthorised use. Privacy helps determine what information a system should share with others with appropriate authorisation. Finally, trust can be represented as a subjective belief of one entity to another in a specific context for a specific time. Trust assists in resolving choices into decisions [11–13]. These are all coupled with the notion of uncertainty. While it is unlikely to determine fully (and quantify) the uncertainty of large-scale dynamic systems, e.g., the IoT [14], more accurate identification and estimation of uncertainties in IoT can reduce the risk and impact of underperformance or unreliable decisions [15]. Thus, to allow for accurate decision making, it is crucial to consider two issues: (i) comprehensive classification of uncertainty in the system, and (ii) characterisation of the impact of uncertainty associated with security, privacy, and trust for a particular task in a given context.

Figure 1 illustrates a conceptual representation of the propagation of uncertainty in a four-layer IoT architecture [5] and shows the association of uncertainty across security, privacy, and trust. Existing work on IoT uncertainty, shown in

Fig. 1 A conceptual representation of the propagation of uncertainty in a layered IoT architecture. Uncertainty can present everywhere surrounding an IoT system and influence the security, privacy, and trust. Uncertainty estimation in the five distinct stages of sense, communication, storage, process and decisions in an IoT pipeline is significant. Therefore, finding a way to select approaches and methods to address uncertainty mitigation is crucial

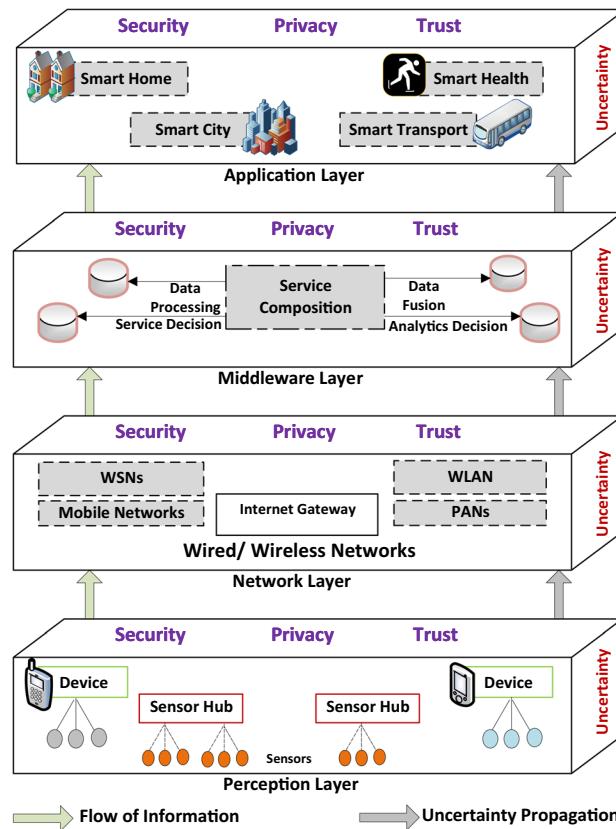


Table 1 (detailed discussion in Sect. 2), classifies uncertainties as either *aleatoric*, arising from noise or randomness in the data, or *epistemic*, arising from a lack of knowledge [16]. While these classes can appropriately characterise uncertainty at a single IoT node, they do not consider i) the distributed nature of IoT networks, ii) the adversarial issues associated with individual nodes or networks, and iii) different impacts that uncertainty has on the security, privacy, and trust. Because of this limitation, existing work is largely unable to represent the complex interactions between uncertainty and IoT security, privacy, and trust, which motivated the focus of this paper.

To address the adversarial issues associated with IoT, we consider *adversarial uncertainty*, which is conventionally considered in machine learning settings, to capture perturbations that arise from malicious actors in the IoT network. The term adversarial uncertainty has been discussed in other disciplines, including deep neural networks and physics [17, 18]. However, in this paper, we introduce adversarial uncertainty in the context of IoT and analyse how it propagates within the IoT pipeline. Our analysis highlights the significance of adversarial uncertainty on security, privacy, and trust in IoT, and the importance of understanding not only the types of uncertainty, but also their propagation pathways. Based on our analysis, we use a case study of smart grids to discuss key considerations and guidelines for moving forward to better estimate and reduce uncertainty in IoT networks, resulting in improved security, privacy, and trust. The main contributions of the paper are as follows:

- We analyse of uncertainty sources in an IoT network. We also consider adversarial uncertainty in distributed IoT networks, and provide a detailed analysis of various types of IoT uncertainties.
- We map the interactions between the three uncertainty classes (i.e., aleatoric, epistemic, and adversarial) and security, privacy and trust in IoT, by mapping the source and propagation of specific uncertainty types to the different stages of sensing, communication, storage, processing, and decision making in an IoT pipeline.
- We derive guidelines to identify, and mitigate the uncertainties in IoT to support more reliable automation with ML, through a smart grid use case. Our guidelines introduce possible approaches to dissociate and reduce uncertainties through trust and reputation approaches in conjunction with emerging technologies, e.g., data trust, blockchain, and verifiable computing.

The rest of the paper is organised as follows. In Sect. 3, we detail the different representations of uncertainty in IoT systems, uncertainty types, and their sources. In Sect. 4, we consider a layered IoT architecture and discuss how the various uncertainty sources propagate through the different layers. In Sect. 5, we provide a comprehensive analysis of the impact of uncertainty on the security, privacy, and trust attributes of an IoT system using a real-world use case scenario of an IoT-enabled smart grid system. In Sect. 6, we discuss a list of mitigation approaches and methods for uncertainty. Finally, we conclude the paper in Sect. 7.

2 Related work

Several proposals discuss the uncertainty in an IoT system. For example, Cofta et al. [3] introduce the NUT (network-uncertainty-trust) model to reduce measurement uncertainty in autonomous hybrid IoT sensor networks. The authors argue that uncertainty arises from varied operating conditions and the quality of measurement nodes, making traditional

Table 1 Previous proposals on IoT uncertainty as compared to this paper

	References	Epistemic	Aleatoric	Adversarial	IoT Layers Considered	Security	Privacy	Trust
[3]	✓	✓	✗	✗	✗	✗	✗	✓
[4]	✓	✓	✗	✗	✗	✗	✗	✗
[5]	✓	✗	✗	✓	✗	✗	✗	✗
[6]	✓	✓	✗	✗	✗	✗	✗	✗
[7]	✓	✓	✗	✗	✗	✗	✗	✗
[8]	✓	✗	✗	✗	✗	✗	✗	✗
[9]	✓	✗	✗	✗	✗	✗	✗	✗
[10]	✓	✗	✗	✗	✗	✗	✗	✗
[Our Work]	✓	✓	✓	✓	✓	✓	✓	✓

statistical approaches less effective. The model leverages socially inspired concepts of reputation, trust, and confidence to evaluate each sensor's node's reliability based on feedback from other nodes. This method allows nodes with low uncertainty to influence data reconstruction more. However, unlike our approach, the authors only consider epistemic and aleatoric uncertainty in the context of trust-based models.

Azemi and Wahid [4] discuss uncertainty in the IoT environment. The authors present different uncertainties in an IoT system caused by data, device, and network heterogeneity. They identify three levels of uncertainty, namely schema mapping, data, and query, which can lead to potential system failures and unreliable information. The authors also review various approaches to managing uncertainty, discussing their efficiencies and limitations across different IoT domains. Cofta et al. [6] discuss uncertainty in IoT sensor networks, offering a structured overview and contrasting these networks with professional measurement systems. They present a socio-technical reference model and a proposed taxonomy of uncertainty, identifying key challenges and advancing the discussion on improving uncertainty management in IoT sensor networks. Magruk et al. [7] discuss the uncertainty surrounding Industry 4.0, which envisions a smart, interconnected world through IoT, cloud computing, and cyber-physical systems. The paper analyzes IoT uncertainties, identifies potential research areas, and addresses challenges to mitigate negative effects in the design and implementation of Industry 4.0. The proposals discussed above (i.e., [4, 6], and [7]) discuss epistemic and aleatoric uncertainties. However, unlike our approach, they do not consider uncertainty propagation in a layered IoT architecture. Furthermore, issues of security, privacy, and trust are not taken into consideration.

Mejia et al. [8] review decision-making methods under uncertainty for IoT scenarios like smart spaces and Industry 4.0, suggesting a new paradigm for modelling human behaviour to enhance resource management. Tissaoui and Saidi [9] explore uncertainty in IoT, specifically in healthcare settings. The paper analyzes factors influencing uncertainty in complex IoT systems and suggests future research directions. Magruk [10] discusses uncertainty in technological megatrends, focusing on IoT in smart buildings. The paper discusses factors contributing to uncertainty in complex, dynamic IoT systems, particularly with big data growth. The study highlights key research areas and proposes ways to address uncertainty in the development of intelligent buildings. The proposals discussed above (i.e., [8, 9], and [10]) focus only on epistemic uncertainty. Once again, unlike our approach, these proposals lack a focus on uncertainty propagation in a layered IoT architecture and do not consider security, privacy, and trust issues, along with the impact of adversarial uncertainties in a layered IoT architecture. While Ismail et al. [5] present IoT uncertainty focusing on a layered IoT architecture, their comparison is limited only to epistemic uncertainty. In Table 1, we show the comparison of the existing works with our work.

3 The uncertainty paradigm

In this section, we define uncertainty, discuss the types of uncertainty and then identify the potential sources of uncertainty in an IoT system.

3.1 Defining uncertainty

There is no singular definition of uncertainty – it depends on context, and can be defined from the perspective of a human, device, system, application, or network [6, 7]. In an IoT context, uncertainty typically describes an inability to predict the true state of a phenomenon with certainty [3, 5–7, 10]. This phenomenon may include the result of an action or decision [5, 7, 10, 19], or a measurement of the physical world [3, 6]. As identified by [19], this definition of uncertainty requires a corresponding 'ground-truth' state. For example, consider a sensor measuring the temperature inside a refrigerated transport truck – the quality of the sensor (i.e., precision, accuracy, resolution) influences the uncertainty in the temperature measurement, where a low quality sensor is less likely to capture the true temperature inside the truck, and therefore is associated with high uncertainty. Notably, the uncertainty in a measurement differs from the accuracy or error of a prediction [3, 6]. In the above example, despite the low quality of the sensor, it may still occasionally produce very accurate temperature predictions. Uncertainty can also be defined from a statistical perspective, where it is viewed as a second-order statistic of a value that can not be determined exactly [5, 6].

Within a multi-component system, uncertainty can propagate between components or processes. For example, if we consider again the refrigerated transport truck, a highly uncertain temperature measurement may generate high uncertainty in the decision of the temperature controller system. In addition to this, uncertainty can be cumulative [20], where individual sources of uncertainty can combine to induce an overall greater total uncertainty in the system. While

uncertainty can be reduced [3, 5, 6], e.g., by gathering more data, it can not be entirely eliminated from a system [19] [5, 10]. In some cases, the presence of uncertainty may even be desirable if it allows for informed actions or decisions – "it is better to be vaguely right than to be precisely wrong" [19].

The literature identifies two potential reasons a system may be unable to confidently predict the true state of a phenomenon – when the system has limited, incomplete or unknown data surrounding the phenomenon [3–5, 7, 10, 20], or when the phenomenon is affected by chance or randomness [6, 10] [7]. In the following section, we will connect these concepts to the different types of uncertainty.

3.2 Types of uncertainty

Across the literature addressing uncertainty, a wide variety of uncertainty categorisations are presented [6, 7, 9, 10, 19, 21–24]. We propose a broad categorization of three specific types of uncertainty that are relevant for IoT systems: (i) *aleatoric uncertainty*, (ii) *epistemic uncertainty*, and (iii) *adversarial uncertainty*. We define these uncertainty types below, and identify related uncertainty types in the literature.

- (i) **Aleatoric uncertainty** refers to uncertainty arising from noise, randomness, or other unquantifiable factors that may affect a phenomenon [16] [5, 6] – the Latin root *alea* refers to a game with dice, and thus a game of chance. Aleatoric uncertainty can be linked to the precision of a sensor, i.e. the repeatability of a measurement. In visual data, it may manifest as motion blur or glare. Similarly, in radio-based localisation, it can manifest as multi-path propagation or non-line-of-sight signals. While aleatoric uncertainty can be estimated or approximated, it is always present and cannot be removed from the phenomena it affects. It is sometimes referred to as statistical uncertainty, variability uncertainty [9] or indeterminacy uncertainty [7], and is related to data uncertainty [19, 21] [22].
- (ii) **Epistemic uncertainty** refers to uncertainty arising from a lack of knowledge or incomplete information [6, 16] [5] – derived from the Ancient Greek *epistēmē*, meaning scientific knowledge. It is often associated with decision-making models, which are subject to epistemic uncertainty when presented with data that is unexpected or has not been encountered before [25]. In contrast to aleatoric uncertainty, it can be completely removed from a system if the system is given enough data or information. Epistemic uncertainty encompasses related uncertainty types including structural uncertainty [9] [10, 24] [7], model uncertainty [19, 21] [22], parameter uncertainty [9, 24] and unknown uncertainty [10].
- (iii) **Adversarial uncertainty** refers to uncertainty arising from the potential action of an adversary or malicious agent upon a phenomenon. For example, adversarial uncertainty may arise in unsecured networks, where it is unclear whether a 'man in the middle attack' has occurred. This type of uncertainty is related to epistemic uncertainty (as well as event uncertainty described by [23]) – it describes a lack of knowledge about whether a malicious agent has performed an action. We make the key distinction that adversarial uncertainty involves a malicious agent, whereas epistemic uncertainty does not.

3.3 Sources of Uncertainty

A source of uncertainty refers to the phenomena or action that introduces uncertainty to a system or process. In this section, we identify 15 potential sources of uncertainty in an IoT setting, based on the three specific uncertainty categories discussed above.

- **Aleatoric Uncertainty**

- (S1) *Noise in the Sensors* – sensors contain a level of noise in the precision of their measurements. This level of noise is often reduced in high quality sensors.
- (S2) *Noise in the Physical Environment* – ambient noise in the environment, e.g., interference in the radio propagation environment, contributes to aleatoric uncertainty.
- (S3) *Network State Uncertainty* – random and dynamic processes in the network, e.g., time-variable radio link state, may result in loss or delay of data/packet loss. This can result in a reduction of the available information capturing the state of the environment.

- **Epistemic Uncertainty**

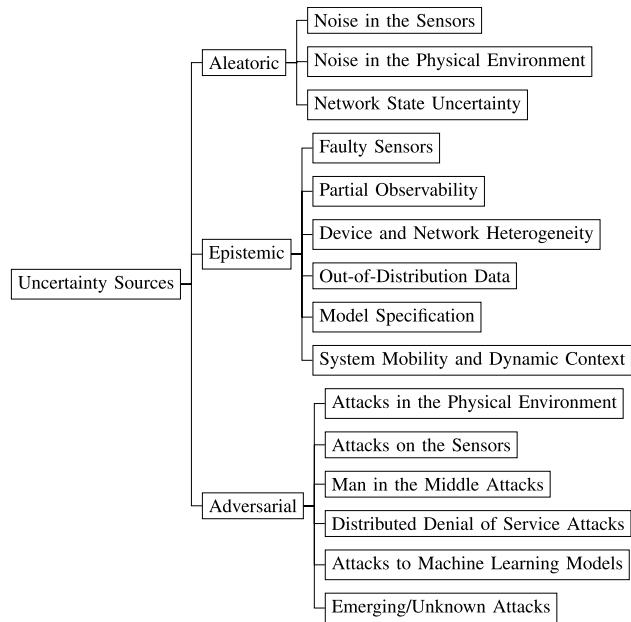
- (S4) *Faulty Sensors* – a faulty or miscalibrated sensor may introduce inaccurate data to the system. The faulty functioning of sensors may also occur by miscalibrating or deploying sensors incorrectly by the people.
- (S5) *Partial Observability* – in IoT, a number of sensors may observe parts of an environment based on their limited field-of-view, which is used to infer the overall state of an environment. This introduces uncertainty around how well the sensor measurements approximate the state of the entire environment.
- (S6) *Device and Network Heterogeneity* – capability, protocol, or software differences in devices and networks can lead to mismatches in data resolution across different nodes, which segregates the environment into areas of lower or higher uncertainty in the physical state.
- (S7) *Out-of-Distribution Data* – anomalous data that is unexpected or does not exist within the typical distribution of data observed for a system may lead to sub-optimal or incorrect decisions. This can particularly be a problem for ML models, which do not generalise well to out-of-distribution data [26].
- (S8) *Model Specification* – in model-based design of systems, we must select an appropriate model for a given task. The choice or specification of a model may introduce uncertainty around how well that model is suited for the respective task and data. This issue of how representative a model is of the underlying environment will always be present, given the abstraction that most models use.
- (S9) *System Mobility and Dynamic Context* – in an IoT system, the state of the physical environment is constantly changing, as is the state of the IoT network. Mobile scenarios lead to an increase in the rate of these changes. This introduces uncertainty around how well the existing data represents the current physical or network state, as well as how accurately we have accounted for context and mobility changes.

- **Adversarial Uncertainty**

- (S10) *Attacks in the Physical Environment* – a malicious agent may change or obscure the environment, thus indirectly affecting the measurements obtained by sensors and introducing uncertainty to the system. For example, an attacker could place a jammer to disrupt wireless transmissions from sensors.
- (S11) *Attacks on the Sensors* – a malicious agent may alter or damage a sensor's hardware or firmware, thus directly affecting the sensor's measurements.
- (S12) *Man in the Middle Attacks* – a malicious agent intercepts communications between two nodes either by secretly eavesdropping or modifying data traffic transferring between them. The agent can sabotage communications with corrupt data (and change the original data traffic) that cause inaccuracy in the measurement value from one node to another. Thus, it increases uncertainty in the resulting decisions.
- (S13) *Distributed Denial of Service Attacks* – a malicious agent can flood the network with malicious traffic to impact the bandwidth or resources of a targeted system. This leads to data unavailability when aggregating measurements, which increases uncertainty in decisions.
- (S14) *Attacks to Machine Learning Models* – a malicious agent may alter the input for an ML model to induce a false prediction. This can either occur by altering the physical environment itself (e.g., in [27]) or by introducing perturbations to the data that is communicated from a sensor to an ML model (e.g., in [28]).
- (S15) *Emerging/Unknown Attacks* – a system can be compromised at any time by unknown attacks. That is, the occurrence and cause of the attack can not be predicted unless the attack has happened (e.g., zero day attacks [29]). Thus, it introduces uncertainty both to the data and networks.

In Fig. 2, we show the different uncertainty sources. We note that this classification of capturing uncertainty and its various sources is beneficial for collecting essential information from the objects (and their corresponding uncertainty values) that will help build an optimal decision. To examine, the significance of the uncertainty types and sources and their mapping to the five distinct stages of sensing, communication, storage, processing and decision-making in an IoT pipeline, we next trace the propagation of these uncertainty types across the layers (and across nodes) of an IoT architecture.

Fig. 2 The sources of uncertainties



4 Uncertainty propagation in IoT

This section discusses uncertainty propagation in IoT systems. In Fig. 3, we illustrate a reference layered IoT architecture and show the propagation of various sources of uncertainties discussed above through the layers that impact security, privacy, and trust in IoT systems. We refer to the three types of uncertainties (i.e., aleatoric, epistemic, and adversarial) and perceive their propagation through the layers. This helps to examine the impact of uncertainty at individual layers and the impact of one or more uncertainties in one or multiple layers. Next, we briefly discuss the layered IoT architecture (cf. Section 4.1) and then explain the propagation of various uncertainty sources through the different layers in an IoT pipeline (cf. Section 4.2).

4.1 Layered IoT architecture

As shown in Fig. 3, we follow a four-layer IoT architecture presented in [5]. It contains perception, network, middleware, and application layers. The perception layer is composed of sensors and actuators that sense data from the physical world. The network layer is responsible for communication among the various components within the system. The middleware layer manages data aggregation and data processing. Finally, the application layer formats the data and provides interfaces for the end-users to access the data.

In the typical sensing, communication, storage, processing and decision stages of an IoT pipeline, sensors in the perception layer *sense* the data from the physical environment. Then the sensed data is moved to the middleware layer through the network layer via an appropriate *communication* medium. Next, the middleware layer *stores* and *processes* the data, e.g., based on the underlying ML models. Finally, the users in the applications layer carry out the *decisions* (in terms of services) for accessing services based on their needs. Next, we show how uncertainty propagates through the different layers in an IoT pipeline.

4.2 Uncertainty propagation

In Fig. 3, we illustrate the propagation of different sources of uncertainties in an IoT pipeline. The aleatoric uncertainties emerge at the bottom two layers of the architecture as they occur due to the errors in the physical environment, device hardware, and network states. That is, they appear at the perception and network layers and go up to the application layer. Adversarial uncertainties appear in all of the layers and go from the lower to upper layers. Finally, the epistemic uncertainties also appear at each layer and move to the upper layers. However, the adversarial uncertainties appear the most compared to the aleatoric and epistemic uncertainties.

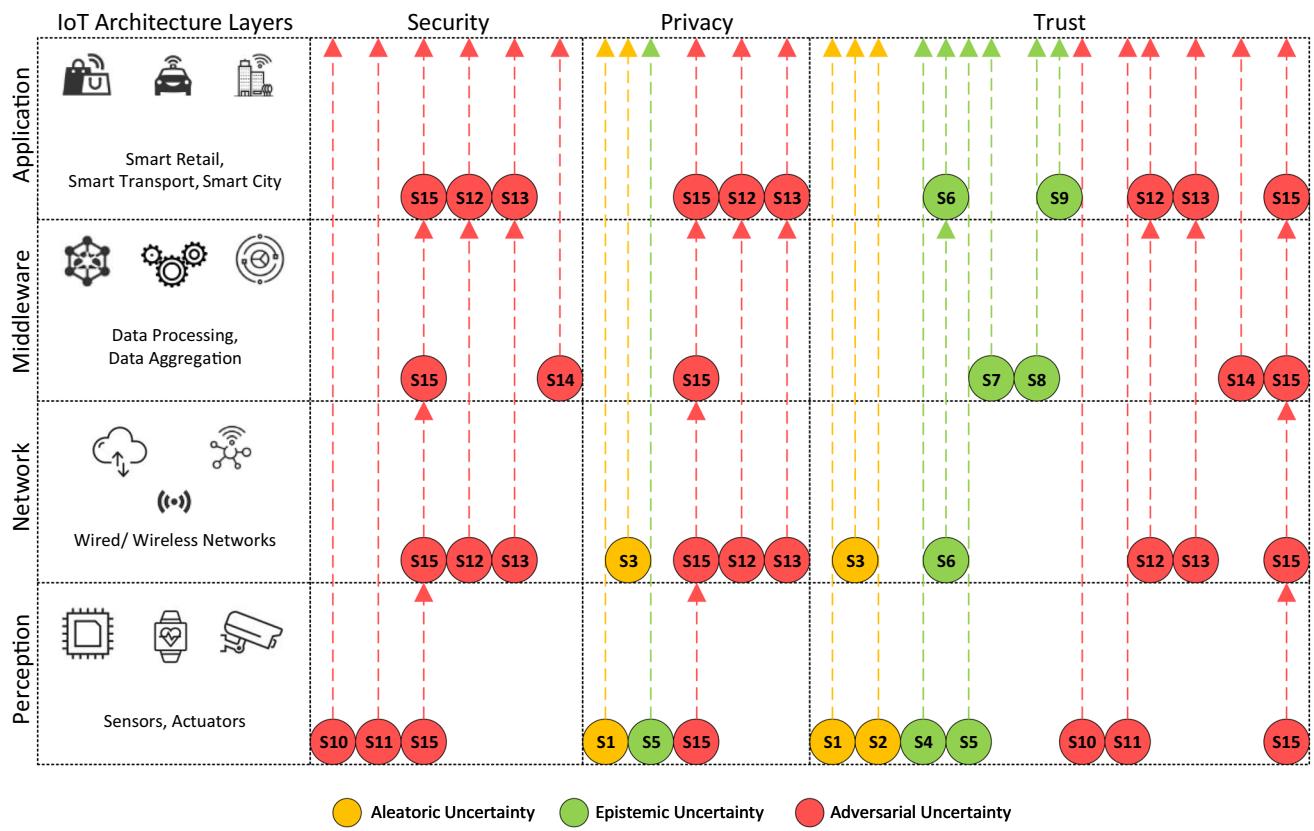


Fig. 3 Uncertainty propagation through different layers of an IoT architecture. We consider three types of uncertainties (and their various sources) that arise at different layers of an IoT architecture. One or more uncertainty can occur at each layer. The uncertainty generated at the lower layer can combine with another newly generated uncertainty at the upper layer during its propagation

We use the term *propagation* to refer to the dissemination of data (i.e., data with uncertainty) within a layer or from one layer to the other. We consider the representation of uncertain data as probability distributions (or estimated values with error bounds) rather than an exact unique value [30]. The propagation can range from simple to complex trends. For example, some uncertainties are introduced in the lower layer and propagate directly to the upper layers or propagate to the same layer, and we call it *single uncertainty propagation*. In contrast, others can combine with another uncertainty and then propagate to the upper layers of the stack or propagate to the same layer, and we call it *combined uncertainty propagation*. The distribution of uncertainties can combine with one or more uncertainties in a single layer or while propagating to the upper layers of the architecture. We also argue that uncertainty can *transfer* from one layer to another. A description of each of these propagation types is given below.

4.2.1 Single uncertainty propagation

Consider an example of an adversarial uncertainty, e.g., attacks on the sensors (S11), occurs only at the perception layer, and propagate to the middleware layer through the network layer, and then propagate to the application layer. Commonly, an adversary can tamper with the hardware or software features of the sensors by their cyber methods that may fundamentally violate the security properties of confidentiality, integrity, and availability through unauthorised access or modification of the underlying sensor's data. The uncertainty caused due to this inaccuracy in the measurements can impact the decision-making models in the middleware layers during propagation, which in turn again may impact the Quality of Information and Quality of Service received by the users in the application layer. In this case, only one source of uncertainty generated at the perception layer propagates from the lower layer to the upper layer.

Now consider a situation where an uncertainty originates and propagates in the same layer. Assume an emerging/unknown attack (e.g., S15) that may come in any form and at any time and originate in a single layer that causes uncertainties to the system and propagates in the same layer [31]. For instance, at the perception layer, smart sensors' hardware

or software features can be tampered with by the attackers generating uncertainties in actual data measurement. In the network layer, a packet dropping attack can lead to packet loss or latency in the communication traffic between the nodes generating uncertainties to access data in transit between the nodes. In the decision layer, an exhaustion attack can interrupt the IoT infrastructure's data processing, generating uncertainties and taking down services or underlying network infrastructure responsible for delivering content. Finally, a social engineering attack can capture and manipulate a user's private information in the application layer generating uncertainties in determining the user's identity, consequently impacting the access to the underlying smart services in the application layer.

4.2.2 Combined uncertainty propagation

The influence of this uncertainty propagation is more significant when impacting the services of a layer. For example, uncertainties due to data tampering in the application layer (e.g., S11), and the packet dropping attacks in the network layer (e.g., S12) can combine in the network layer and propagate to the middleware layer. This combined uncertainty may cumulatively impact data quality which disrupts the underlying ML model's performance in the middleware layer to a larger extent [32]. Note, in this example, two same types of uncertainties (i.e., adversarial uncertainty) generated in two different layers of the stack propagate from lower layers, combine in an upper layer, and then propagate together. In other cases, two different uncertainties can combine and propagate together. For instance, an aleatoric uncertainty (e.g., S1) generated in the perception layer can combine with an adversarial uncertainty (e.g., S15) in the network layer and then propagates together to the middleware layer. Similarly, an epistemic uncertainty generated in the perception layer due to the faulty sensors (e.g., S4) can combine with an adversarial uncertainty due to the attacks on the ML models (e.g., S14) in the middleware layer and jointly propagate up to the application layer.

Now consider a situation where two (or more) different (or similar) types of uncertainties are combined and propagate in one layer. For instance, the uncertainty generated due to the sensors' failure (e.g., S1) can combine with another uncertainty caused due to the partial observability (e.g., S5) in the perception layer and propagate in the same layer.

A similar trend can be seen for all other sources of uncertainties in different layers, along with their impact at each layer during a combined propagation through the IoT pipeline. However, such a combination of uncertainty can be purposeful by the attackers or non-intentional. How and when uncertainties can be combined (resulting in the sum or bigger than the sum) for final decision-making remains an open research issue. Further, the deterministic comparison of the impact of propagation for such combined value of the same sources of uncertainties (e.g., adversarial) versus the different sources of uncertainties (e.g., adversarial and epistemic) remains another open research issue.

4.2.3 Uncertainty transfer

Note that uncertainty can *transfer* from one layer to another without impacting the system's performance, particularly when the uncertainty is hidden through encapsulated fields in packets that traverse layers. We, therefore, distinguish between the *transfer of uncertainty*, where it is simply relayed from one layer to another layer, and the *propagation of uncertainty*, where uncertainty at one (or multi) layer can cause impacts to the system's performance. For instance, an uncertainty generated in the perception layer (e.g., S1) transfers through the network layer, and propagates to the middleware layer by impacting the system's security, privacy, and trust in the middleware layer (refer to more discussion in Sect. 5). However, in which context an uncertainty will propagate and transfer remains an open research issue.

4.2.4 Summary of uncertainty propagation and transfer

We find that sources of uncertainty can be introduced at every layer of an IoT architecture. The adversarial uncertainty is more prominent for security, privacy, and trust than aleatoric and epistemic uncertainties. We see all of the three uncertainty types impact trust, and to a lesser extent, privacy.

Significantly, we also introduce a key distinction between uncertainty propagation and transfer. We consider propagation impacts the layer's functionality, but transfer simply transports the (amount of) uncertainty from one to the other layer. We also note that the network layer performs the transfer of uncertainty primarily. However, quantifying the impact of the uncertainty is challenging as it depends on several factors, e.g., the quality of input data, the context of the system, complex network dynamics in different protocols, etc., and therefore, we argue uncertainties can be observed but can not be eliminated completely. In the following section, we provide a comprehensive analysis of the impact of three types

of uncertainties (i.e., aleatoric, epistemic, and adversarial) mentioned above in an IoT pipeline for security, privacy, and trust attributes using a real-world smart grid use case scenario.

5 Impact of uncertainty propagation

In this section, we discuss the impact of uncertainty in an IoT system based on the three major attributes – security, privacy, and trust. We examine these attributes based on the underlying sources of uncertainties (discussed in Sect. 3) at each layer of the IoT architecture (discussed in Sect. 4.1). We find that with the increased level of three types of uncertainties (i.e., aleatoric, epistemic, and adversarial), security and trust decrease within the system. Interestingly, in general, privacy increases with the increased value of aleatoric and epistemic uncertainties. It is possible that an adversary intentionally injects noise to create a false sense of privacy and then removes the noise to recover the private data. Here, privacy decreases with the increased level of adversarial uncertainty. Below, we employ an example smart grid use-case to discuss these impacts in detail in a real-world setting.

5.1 An example use-case

We employ a use-case scenario of an IoT-enabled smart grid system [33] to demonstrate various sources of uncertainty and outline the impact of such uncertainty on the security, privacy, and trust attributes. In Fig. 4, we depict a general overview of a smart grid. The penetration of the renewable energy sources, along with a two-way communication model, transfers the conventional energy consumers to energy prosumers who are not only consumers but also producers of energy that can be injected into the grid. Consider a smart home equipped with solar panels as an example of an energy prosumer. The solar panels generate energy to power the home during daylight and the excess energy is injected into the grid. During the night time, the home turns into a pure consumer that consumes energy from the grid [34]. Each smart home is equipped with a Building Energy Manager (BEM) that manages and controls the energy consumption of the house by predicting the future energy demand/generation. BEM also attempts to balance the load and reduce the energy cost by scheduling the operation of appliances based on the energy price.

Virtual Power Plant (VPP) is another example of energy prosumers [35]. A VPP is a combination of various grid participants that share the same features, e.g., solar panels, or smart homes, and are represented as a single entity in the smart grid, known as a VPP manager. The latter collects and aggregates the energy consumption/generation of the underlying nodes and informs the grid operator. Any changes to the predicted value can be managed by adjusting the load/generation of other nodes in the VPP, thus ensuring that the total load/generation remains stable.

Referring to the layered IoT architecture (shown in Fig. 3), underlying sensors (e.g., solar panels, smart meters, or home appliances) collect (*sense*) energy generation/consumption data from the physical environment and send it to the grid

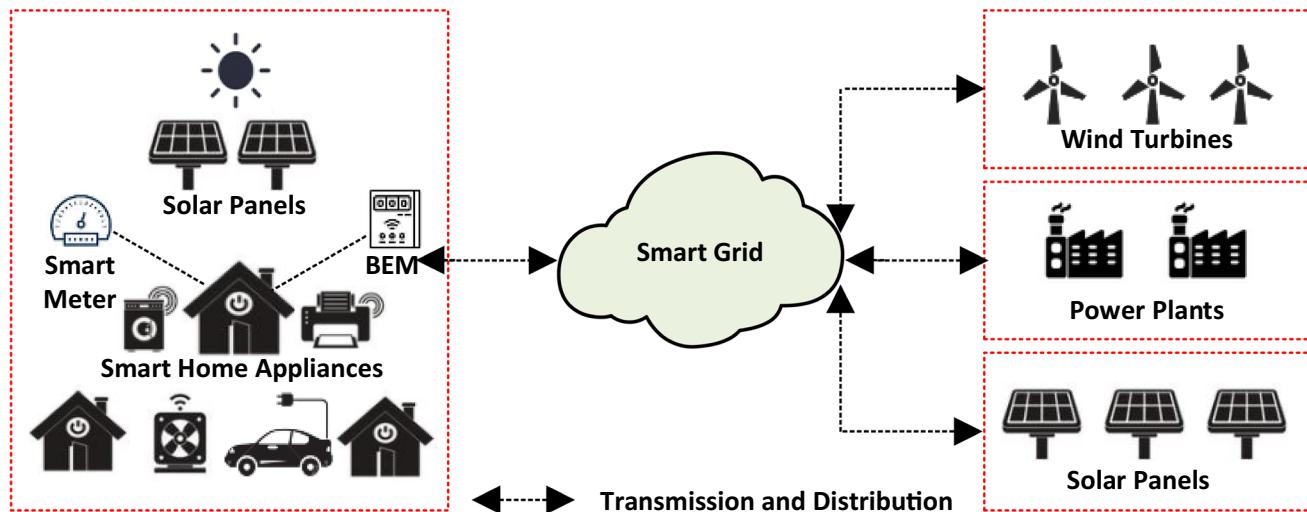


Fig. 4 An illustration of IoT-enabled smart grid system

operators through the network layer. It allows a two-way *communication* between the power grid and end customers with emerging needs to monitor, predict, plan, learn and make decisions about energy consumption and production in real-time [36]. For example, in such an IoT-enabled smart-grid system, the BEM manages the stability between supply and demand among the various household appliances in a particular building by periodically *processing* the data sensed by the solar panels and smart meter and taking appropriate *decisions*. The processed data can be stored in an appropriate *storage* by the BEM before it sends the data to the grid operator. Simultaneously, the grid operator also processes the received data and makes appropriate *decisions* to track energy consumption and predict future energy demands and costs. Appropriate ML models are used by the grid operators located at the middleware layer to make price and energy predictions and detect anomalies autonomously based on the available data. BEM can also have its ML model (for instance, located in the middleware layer) for predicting energy consumption and future energy demand for home appliances. Finally, smart grid participants, e.g., smart home devices, in the application layer use the relevant services, e.g., purchase or trade.

For reliable operation of the smart grid, security, privacy, and trust need to be ensured both at the physical and cyber levels. Different types of cyber attacks, modification of private information, non-trusted data sources, inaccurate data measurement, and inefficient decision-making could introduce uncertainties that may hamper the stability while causing load imbalance in the smart grid system.

In Fig. 5, we show the interactions among the different entities in an IoT-enabled smart grid system. We map the distinct stages of sense, communication, storage, process, and decision-making in an IoT pipeline (in dotted boxes) where potential uncertainty can arise. It is essential to detect and mitigate uncertainties in each of these stages to reduce energy waste, determine accurate energy pricing, and ensure reliability and stability for the grid. Next, we discuss the impact of uncertainty on the security, privacy, and trust against the IoT-enabled smart grid application use-case discussed above.

5.2 Security

Security ensures that the information should not be exposed to an unauthorised user by maintaining authentication, reliability, non-repudiation, and accountability [37]. In addition, it supports the confidentiality, availability, and integrity of the information [38]. In Fig. 3, we see that only the adversarial uncertainties have significant consequences and impact security issues in an IoT context. Commonly, the level of security decreases with the increase of uncertainty in the system. In other words, a system with higher uncertainty is less secure than a system with lower uncertainty.

Some notable sources of adversarial uncertainties that impact security, among others, are attacks on the physical environment (S10), attacks on the sensors (S11), and emerging/unknown attacks (S15). For example, in the IoT-enabled smart grid context, attackers can disconnect multiple solar panels to stop working (i.e., in the perception layer of an IoT stack), which impacts capturing the accurate measurements of the sensors (i.e., the actual energy generation). Furthermore, the uncertainty generated in the perception layer can propagate to the upper layer (i.e., to the middleware layer). The grid operator utilises such measures to predict future energy consumption/generation and determine the energy price. Thus, propagation of uncertainty with tampered data results in an unbalanced energy grid, and it can cause inaccuracy in the energy distribution. Similarly, an attacker can compromise the smart meters and thus tamper with the energy generation/consumption measurements injected into the grid.

From an adversarial point of view, an attacker can control one or multiple devices to disrupt the smart grid system's functionality. For instance, an attacker can penetrate a user's home network and take unauthorised control of the devices, e.g., a smart refrigerator. The attacker can increase and decrease the cooling temperature of the refrigerator frequently. As

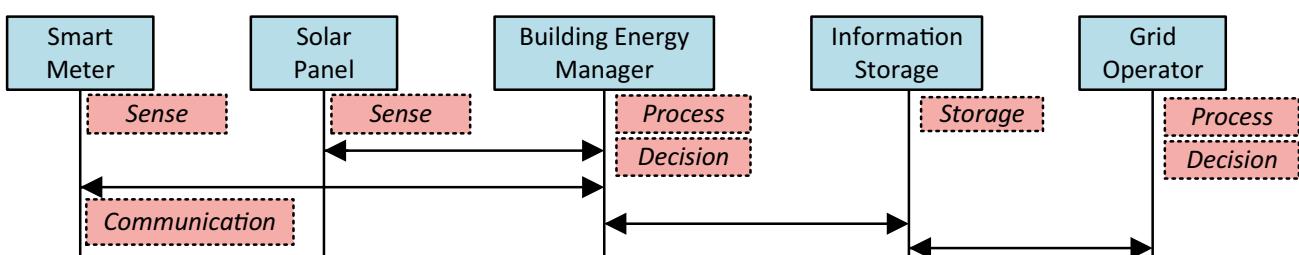


Fig. 5 Interactions among the various entities in an IoT-enabled smart grid scenario. We map the five distinct components (i.e., sense, process, storage, communication, and decision) in an IoT-enabled smart grid scenario. The dotted boxes represent these components where potential uncertainties can arise. Note that all bidirectional arrows represent communication

a result, the generated uncertainty due to inaccurate data measurement can imbalance the functionality when propagating to the other components (e.g., the BEM) for determining a stable energy consumption for a certain period. In an IoT pipeline, in the perception layer, attackers can gain unauthorised control of one IoT device and infect many connected IoT devices (by black-hole and worm-hole attacks) to manipulate inaccuracy in measures in energy consumption on a large scale [39]. These inaccurate data measurements are then propagated to the middleware layer through the network layer. In the middleware layer, the underlying ML models make decisions with the propagated uncertainty present in the data. Similarly, in the IoT-enabled smart grid context, an attacker can gain unauthorised access to large numbers of solar panels or smart home appliances and produces inaccurate data measurements that provide incorrect information on actual energy generation in a certain period. Once again, these incorrect data can cause uncertainty for the energy grid by generating exaggeration in ML models in the energy distribution/prediction. We note that adversarial uncertainty occurring from emerging/unknown attacks (e.g., S15) has a higher impact on the system from a security point of view as it originates at each layer of an IoT architecture.

5.3 Privacy

Privacy deals with the legal and non-legal norms regarding the disclosure of information of one party to another [40]. Privacy preservation mechanisms rely on standard policies and processes to provide restrictions, legitimacy, and transparency in information sharing [41]. In an IoT context, we observe that uncertainty and privacy are closely coupled. For instance, higher aleatoric or epistemic uncertainties in a system enhance privacy by making it more difficult for an attacker to extract sensitive data. This can be done by employing obfuscation techniques to control information disclosure. For example, proposal [42] shows that purposefully increasing aleatoric uncertainty makes it harder to classify IoT devices by unauthorised entities, contributing to greater privacy. However, we note that privacy decreases with the increased level of adversarial uncertainties, where attackers may gain access to sensitive information.

That said, the data with high uncertainty is more private, especially when considering aleatoric and epistemic uncertainties. Therefore, higher uncertainty within a data source can be more effective in privacy protection and accountability of data leaks. For instance, a smart meter periodically sends energy reports to the BEM over wireless communication. An eavesdropper can intercept such reports to invade consumers' privacy, for example, what time the property is occupied or empty, further introducing privacy issues to the individual's life patterns. However, increased uncertainty in the energy reports makes it difficult for an attacker to accurately interpret a consumer's household activities.

However, to achieve privacy, there is a trade-off between security and trust. For instance, an increase in uncertainty to achieve higher privacy decreases the system's security and trust. We argue that it is important to consider whom and how much data should be shared from the data source's perspective. At the same time, a data receiver must consider the QoL received from a data source resulting in a QoS [43]. Thus, the uncertainties between the source and the receiver create an ambivalence fundamental to the privacy issue. For example, in an IoT-enabled smart grid context, the BEM must send the actual measurement of power consumption of the smart home to the grid operator, ensuring QoL. However, it needs to keep the other information hidden (e.g., the device names and their energy usage patterns) from the grid operator. Then, the grid operator must predict an ideal energy distribution/price resulting in QoS without revealing individual household information. This can be achieved, among others, using *unlinkability* (i.e., the incapability of stating the association between two observed items of the system) and *undetectability* (i.e., the data should be undetectable to the adversary) [44].

In the depicted IoT layers in Fig. 3, we observe that the three types of uncertainties (i.e., aleatoric, epistemic, and adversarial) have impacted privacy. However, the adversarial uncertainty is most prominent in all layers, as it occurs at every layer in an IoT architecture. Thus, the adversarial uncertainty has significant consequences on the performance of IoT systems during its propagation. For example, in the IoT-enabled smart grid context, an adversarial uncertainty caused by an emerging/unknown attack (S15) by gaining unauthorised control of the sensors in a smart home can cause data tampering by deliberately modifying, destroying, manipulating, or editing the data. This can reveal sensitive information (e.g., energy consumption rates of individual devices) through unauthorised channels to the attackers during its propagation, compromising the user's privacy (or user's to a greater extent) by disclosing the sensor data. Due to the high temporal and spatial granularity, data coming from sensors offer great potential for data mining, making it difficult to preserve privacy. For example, as mentioned earlier, smart meters collect a temporally fine-grained report of energy consumption in the smart grid context. It allows the utility to estimate better the domestic power consumption leading to optimised distribution and control of the grid. However, an adversarial attack can gain unauthorised access to the sensitive inferences, e.g., occupancy and lifestyle patterns of the occupants from the data in addition to total power

consumption and generate an imbalance in the smart grid system by inaccurate data processing. Once the attacker has such private information, in the later stage, attackers can propagate uncertainty created due to the falsified information of a particular household (altering the actual data) to the grid operator, ultimately producing an incorrect energy generation/price prediction creating uncertainty in decision-making for energy distribution [45].

5.4 Trust

Commonly, trust determines what level of information that must be measured to the confidence and risks associated with the particular interaction between the trustor (i.e., who is trusting) and the trustee (i.e., who is being trusted) within a specific context [46]. In a large-scale IoT system, trustors and trustees need to make autonomous decisions based on the input data from different uncertain sources [47]. Hence, aggregating data from multiple uncertain sources compounds uncertainty and makes trusted decision-making more challenging.

In Fig. 3, we see that the three types of uncertainties impact the trust in the IoT systems – adversarial has the highest occurrences, followed by epistemic and aleatoric. Significantly, with the increase of each uncertainty, the trust decreases. This is because uncertainty decreases the confidence level for decision-making between the trustor and the trustee. This confidence level helps to measure the overall trust [48].

We note, among others, that in the IoT perception layer, notable sources of aleatoric uncertainties are noise in the sensors (S1) and faulty sensors (S2). In the middleware layer, substantial epistemic and adversarial uncertainty sources are model specification (S8), attacks to ML models (S14), and emerging/unknown attacks (S15). In the employed IoT-enabled smart grid context, unwanted noise in the sensors (in the solar panel) can lead to the inaccurate measurement of the actual data value. For example, the noise created due to the cloud covering the solar panels generates inaccuracy in measurement. Therefore, it creates uncertainty for the device's trust when the measured values propagate from the devices to the smart home BEM (and extends to the energy grid operator) when aggerating the energy consumption. This is also true for the measurements coming from faulty sensors due to the epistemic uncertainty (e.g., S4) in the system.

Smart sensors (for instance, installed in the BEM) periodically send the measured energy consumption to the grid operator. For the grid operators, a trustworthy data source is expected to get QoI and, in turn, provide high QoS. However, it is challenging for the grid operators to trust the information that the BEM dictates. For instance, having been compromised by the man-in-the-middle attacks (e.g., S13), causing adversarial uncertainty, a compromised BEM can send falsified information to the grid operator with less energy consumption, leading to uncertainty towards the price prediction. Thus, this uncertainty amplifies the challenge of data trust in the system. Furthermore, the uncertainty generated due to the falsified data (e.g., S4) in the perception layer can propagate to the middleware layer. The propagated uncertainty can impact the ML models (by training and recognizing specific patterns) running inside the grid operators to predict the energy demand when balancing the energy distribution, leading to uncertainty in the model trust in the system.

5.5 Summary

Our extensive analysis using a real-world use case scenario of a smart grid system shows that uncertainty propagation significantly impacts an IoT system's security, privacy, and trust issues. To mitigate uncertainty, a list of approaches and methods is necessary. However, several open issues must be taken into consideration. For instance, whether employing single or multiple mitigation techniques for one or more sources of uncertainties and quantifying the data with a high degree of confidence at each layer of an IoT pipeline, mainly when a system deals with a series of inconsistent data. This leads us to explore a list of potential approaches and methods for uncertainty mitigation discussed in the next section.

6 Mitigating uncertainty propagation

As discussed previously, uncertainties in the IoT pipeline may occur from various sources and impact the system's overall functionality. In fact, uncertainties will always be present in the system, and in this section, we aim to guide mitigation strategies rather than eliminate uncertainties. However, there is no complete and specific mitigation technique to address uncertainty as a whole. The appropriate mitigation strategies for uncertainties will depend on the system's requirements and the designer's choice.

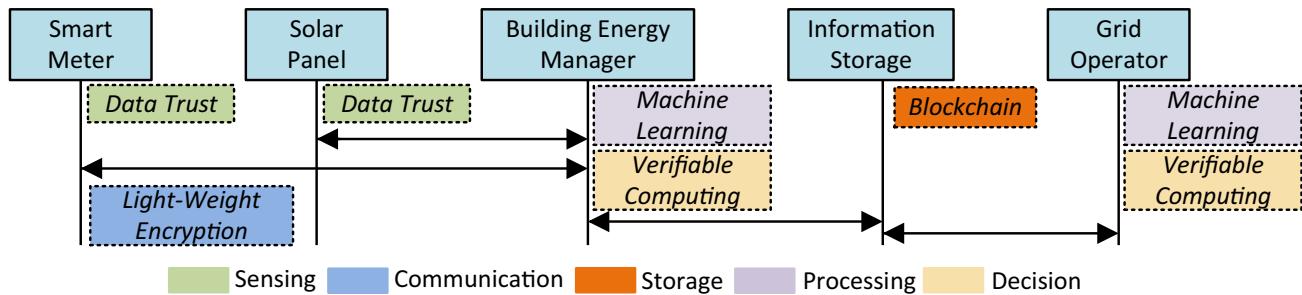


Fig. 6 Potential approaches and methods for mitigating uncertainty in an IoT-enabled smart grid scenario. The dotted boxes represent the potential mitigation approaches and methods to sources of uncertainties that are depicted in Fig. 5

Table 2 We show the five distinct stages within the IoT-enabled smart grid use case scenario, along with potential uncertainty mitigation techniques

Stages	Sensing	Communication	Storage	Processing	Decision
Mitigation Tech-niques	Data Trust [55] [56, 57]	Data Trust [55] [56, 57]	Machine Learning [60–63]	Blockchain [68–70]	Machine Learning [60–63] Verifiable Computing [71–73]

In order to provide approaches and methods for mitigating uncertainties in a more granular way, we examine and map the five distinct stages, i.e., sensing, communication, storage, processing, and decision-making as illustrated in Fig. 5, in the employed IoT-enabled smart grid use case scenario. Note these components are conceptual, and they can easily be distributed and integrated into the different layers of an IoT pipeline. Here, we discuss how various approaches and methods can be employed to mitigate uncertainty in the IoT-enabled smart grid use case scenario.

The security approaches in IoT network communication are widely discussed. For instance, light-weight cryptographic protocols for IoT communication are presented in [49, 50], and [51]. Therefore, apart from the general security issues in IoT network communication and the physical security concerns of the entities (e.g., solar panels, smart meters, BEM, etc.), there are four aspects that must be considered when providing approaches and methods for mitigating uncertainties: (i) to quantify the trustworthiness of various data sources, e.g., certain trust level of various entities that report information is not the same, (ii) a distributed and decentralised data-sharing platform that can perform computation at scale in a trustless environment, (iii) efficient detection and prediction of abnormal behaviour of an entity or process to create accurate models to guide future actions, and (iv) verify the correctness of computing nodes, where information may have been derived from a number of processes.

For sensing, the aforementioned discussion reflects that uncertainty can be addressed by employing the appropriate *data trust models* in the sensing process. The model can select the more reliable and trusted data sources to recognise patterns and then make predictions. Recall that more trusted data leads to reduced uncertainty. For storage, *blockchain* is a distributed ledger that can provide a solution for storing data using strong cryptographic mechanisms and overcoming the need for a centralised trusted authority. For processing and deciding, *ML* provides improved automation through experience and by the use of data. Finally, *verifiable computing* can verify the process, and, therefore, verify the integrity of the processed data. Verifiable interactions can assure that the interactions had happened between two entities when composing a derived (or indirect) trust performance. Next, we discuss how these various approaches and methods can help mitigate uncertainty propagation and address the security, privacy, and trust issues. In Fig. 6, we illustrate such mitigation approaches and methods (in dotted boxes). In Table 2, we summarize the uncertainty mitigation techniques within the IoT-enabled smart grid use case scenario.

6.1 Data trust

Commonly, uncertainty is a significant cause of poor data quality. Two fundamental issues are: (i) the selection of two or more data sources based on the level of uncertainty present in those sources, and (ii) quantifying the level of uncertainty in the data provided by these sources. These issues precisely form the core motivation for selecting an appropriate data trust model. To address the first issue, two potential approaches can be applied. First, entities (e.g., smart meters, solar panels) collect information from all possible sources and then perform majority voting to select the best possible data. Second, a trust threshold is used to select the data sources based on the previous interactions. Although these approaches intend to address the trust-related issues, they do not fully address the uncertainty issues as they do not use any mechanism to measure the uncertainty in the data.

The second issue is more related to the data uncertainty (that relates to QoI). In general, data collected from the sources may contain uncertainty of different types discussed above. To provide a better system's functionality, minimising uncertainty is important. It helps quantify how close the information is to the actual value. Conversely, high uncertainty reflects that it cannot guarantee the truthfulness of data. Using appropriate data trust models can provide some confidence to reflect/integrate different uncertainties to provide better QoI. Returning to our use-case scenario of a smart grid, the selection of data trust models is significant for smart meters and solar panels. Because these two entities are responsible for sensing information and placing proper data trust models will guarantee the trustworthiness of different data sources [52].

In [53], the authors propose a data trust model that follows semantic modelling of the data sources and their respective levels of trust. The model can also capture the degree of uncertainty of this data. In [54], the authors present a distributed trust management framework using fuzzy logic. Other approaches, e.g., [55, 56] and [57], provide data trust models that can provide efficient performance in distributed system environments. In the smart grid use-case scenario, these approaches can potentially be applied to mitigate uncertainty by selecting more trusted data sources for solar panels and smart meters.

6.2 Machine learning

As explored in Sect. 3.3, ML models are prone to all three types of uncertainty – aleatoric uncertainty when processing noisy data from a sensor (S1), epistemic uncertainty when encountering data outside their learnt distribution (S7), and adversarial uncertainty when processing data tampered with by an adversarial attack (S14). In the ML literature, the field of uncertainty estimation enables ML models to estimate the presence of different types of uncertainty, which can then be output alongside their usual prediction (see [26] for a survey on common approaches to ML approximating uncertainty). This provides the ML model, and all subsequent components of the system, with an awareness of the uncertainty currently present at that level in the system.

Given a ML prediction with estimating high uncertainty, a subsequent decision-making process can choose to act cautiously, e.g., gathering more data, or ignoring the prediction altogether. While this does not remove or eliminate uncertainty from the system, the potentially negative effects of uncertainty can be mitigated by allowing for more informed and reliable decision-making. This estimated uncertainty becomes even more informative when the ML model can distinguish between the types of uncertainty, as this provides information about the impact on the security, privacy and trust of the system.

In the smart grid scenario discussed above, ML models can be applied in many places [58]. For example, in BEM, energy consumption is measured and predicted based on the available information coming from solar panels and smart meters. Additionally, smart grid operators may use ML to predict future energy consumption depends on the currently available information. These ML models typically rely on supervised ML, whereas unsupervised ML can also help create energy demand profiles through clustering. Reinforcement learning algorithms are also applied to make energy dispatch decisions and activate demand management signals to maintain the balance of power supply and demand [59]. Each of these applications of ML in the smart grid scenario has the potential to introduce uncertainty into the system – for example, uncertainty about the specification and suitability of the chosen ML model for the prediction task. However, they also offer the potential to estimate the existing uncertainty at the relevant step in the smart grid system.

A number of works have highlighted the potential of uncertainty estimation in ML models for smart grid scenarios [60–63]. In [60] and [61], load forecasting is performed by an ML model that also can predict epistemic uncertainty.

Through the application of Bayesian Deep Learning techniques, the ML models can accurately predict the future load, as well as a variance in that prediction (representing the model's uncertainty in the prediction). Both [62] and [63] propose ML algorithms for detecting false data injection attacks in the smart grid. By predicting the presence of a malicious attack, these works mitigate and identify adversarial uncertainty present in the system. Specifically, in [62], a Dynamic Bayesian Network is employed to detect unobservable cyber-attacks in real-time, using free energy as an anomaly index. By identifying adversarial uncertainty in the system data, these approaches help to eliminate incorrect data and improve prediction accuracy, while also warning of the presence of malicious entities.

6.3 Blockchain

Blockchain provides a decentralised infrastructure for multi-stakeholder applications where the digital data is shared among the stakeholders through middleware [64]. Moreover, distributed consensus mechanism of blockchain can verify the digital data agreed upon by multiple stakeholders. After validating digital information, the information is stored in the immutable digital ledger, which is impossible to tamper with. This data is reliable, and transactions are traceable to the underlying accounts. In the context of a large-scale distributed system like the IoT, it helps to reduce data redundancy when collecting data from multiple stakeholders. Which in turn reduces uncertainty in the data processing.

In the smart grid scenario, the use of blockchain for storing information is beneficial for data integrity. Blockchain increases the transparency between stakeholders, ensures data security and privacy in a trustless manner, simplifies the energy demand and supply chain, and minimises distribution losses [65]. There are several practical deployments of blockchain-based platforms to mitigate data redundancy for smart grids. For instance, 'Brooklyn Microgrid' [66] and the 'Electron project' [67] allow local solar energy consumers to exchange data through blockchain. These blockchain-based platforms facilitate grid operators, users, local energy markets, and distributed energy sources to participate in numerous grid optimisation demands with diverse energy assets.

Different blockchain-based approaches have been proposed to provide security, privacy, and trust in the smart grid use case. For example, a Privacy-Preserving Energy Transactions (PETra) approach proposed by [74] provides anonymity for communication, bidding, and trading using smart contracts. In [75], the authors propose a permission-based blockchain model for smart grid networks to ensure data privacy and energy security by protecting manipulation of stored data. Other works, e.g., [76–79] discuss the need for lightweight security solutions for advanced metering infrastructures to prevent man-in-the-middle attacks and data tampering through timely adversarial node detection, localisation, and provenance through blockchain. Blockchain-based solutions are also used to provide trust management for the smart grid system. For instance, proposals [68] and [69] discuss a multi-agent trust management framework for the smart grid using blockchain. The proposals use different trust evaluation methods (e.g., trust distortion, consistency and reliability) from different trust evaluators to compute the overall trust score of the system. Furthermore, the employment of block-chain smart contracts reduces data inconsistency (i.e., stored data is immutable and permanent), and therefore, helps mitigate uncertainty at some level [70].

6.4 Verifiable computing

Data processing is one of the fundamental operations in multi-layered IoT systems. As the information gets exchanged among layers, it gets processed or aggregated. In some cases, ML models generate insights from the data. All this processing involves computations on data. Computations may produce faulty results due to either adversarial attacks (e.g., S13 and S15) or inherent hardware failures (e.g., S4), introducing uncertainty to the system [80].

Proposal [71] introduces a technique to validate the correctness of computation by gathering run-time traces from the computing environment. Note that processing techniques repeatedly run in IoT applications. For example, new sensor data from lower layers triggers a particular processing software in the middleware layer. Given the repetitive nature of the processing operations, the system can employ verifiable computation to generate a run-time trace agnostic to the data inputs. In other words, a processing uncertainty mitigation technique can be developed by verifying the consistency of run-time traces. Correct execution of data processing will produce a valid and auditable trace, providing a verification mechanism to the system. Any variations in run-time trace would signal suspicious operations, which will allow the system to detect and prevent uncertainty propagation.

Verifiable computation is based on remote audits [72] that can be seen as a viable alternative for cryptographic approaches. Following this approach, a computing platform submits a proof in the form of run-time traces and stack profiles to prove to the verifier that it has executed the computations correctly. vPython is an open-source

software [73] that allows any computer to prove to the verifier that it has executed a Python-based computation correctly by providing run-time traces and stack profiles. vPython verifies and ensures software correctness, which would help the application developers identify uncertainties or other vulnerabilities.

The use of verifiable computing during the decision processes would be beneficial in verifying the consistency of run-time traces in a smart grid scenario. It is useful, for instance, when making more accurate energy consumption decisions by the BEM and the grid operator. In addition, verifiable computing can automatically detect run-time errors, e.g., memory access errors and memory leaks that may be induced due to some uncertainties in the smart grid. This process will scale up relatively well and give more confidence in the analysis results to determine if the non-trusted software operates correctly while providing auditability.

7 Conclusion and future work

In an IoT system, a vast amount of data is collected, processed and propagates to the various layers of the architecture. This data is collected and shared among the entities, often in uncertain conditions. This leads to the growing concern of uncertainty present in the data. A study on uncertainty comprising a detailed investigation of sources and types of uncertainty to examine the impact of uncertainty propagation on security, privacy, and trust attributes in an IoT system is craving the present literature. In this paper, we illustrated how uncertainties arise, propagate and examined their impact on security, privacy, and trust attributes in an IoT pipeline. We presented a comprehensive description of two known uncertainty types, namely, aleatoric and epistemic, along with their various sources in an IoT system. Further, we introduced a novel category of uncertainty for the IoT, called adversarial uncertainty. We highlighted how the different sources of uncertainty propagate in an IoT pipeline and their associations to security, privacy, and trust goals. We noted that only the adversarial uncertainty impacts security, and it also has a more significant impact on both privacy and trust. Aleatoric uncertainty impacts privacy more than trust, and epistemic uncertainty affects more trust issues than privacy. To mitigate uncertainty generated in an IoT system, we discussed approaches and methods, including data trust, machine learning, blockchain technology, and verifiable computing. We observed that it is challenging to provide a unique solution for each type of uncertainty with the above approaches. On the one hand, a mitigation approach or method can handle multiple uncertainties and work at various layers in an IoT pipeline. On the other hand, a combination of approaches and methods may be required to address a single uncertainty. However, the selection will depend upon the system's requirements and the designer's choice. The quantification of IoT uncertainties discussed in this paper, in a real-world setting, and the measurement of such propagation, along with impact assessment, remain open research issues for future work.

Author contributions S.P., Writing Original Draft, Investigation, Validation, Methodology, Conceptualization. Visualization. S.K., D.M., and V.D., Resources, Methodology, Conceptualization. G.R., and A.D., Review and Editing. P.M., B.K., and R.J., Resources, Investigation, Review and Editing. All Authors Reviewed the Manuscript.

Data availability No data generated for this study.

Declarations

Competing interests The authors declare no competing interests.

Open Access This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

References

1. Tandon A. "Survey of security issues in cyber-physical systems. Cham: Springer; 2022.
2. M. Heydari, A. Mylonas, V. Katos, E. Balaguer-Ballester, V. H. F. Tafreshi, and E. Benkhelifa, "Uncertainty-aware authentication model for fog computing in iot," in *2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC)*. IEEE, 2019, pp. 52–59.
3. Cofta P, Orłowski C, Lebiedź J. Trust-based model for the assessment of the uncertainty of measurements in hybrid iot networks. *Sensors*. 2020;20(23):6956.
4. Azemi NLM, Wahid N. Uncertainty in internet of things: a review. *Int J Adv Technol Eng Exploration*. 2021;8(75):422.
5. Ismail S, Shah K, Reza H, Marsh R, Grant E. Toward management of uncertainty in self-adaptive software systems: iot case study. *Computers*. 2021;10(3):27.
6. Cofta P, Karatzas K, Orłowski C. A conceptual model of measurement uncertainty in iot sensor networks. *Sensors*. 2021;21(5):1827.
7. Magruk A, et al. Uncertainty in the sphere of the industry 4.0-potential areas to research. *Busi Manage Educ*. 2016;14(2):275–91.
8. N. A. Mejía, G. S. Boada, and J. R. de Almeida Amazonas, "Decision making under uncertainty for the deployment of future networks in iot scenarios. Springer: Cham. 2020.
9. A. Tissaoui and M. Saidi Uncertainty in iot for smart healthcare: Challenges, and opportunities. Springer: Cham. 2020,
10. Magruk A. The most important aspects of uncertainty in the internet of things field-context of smart buildings. *Procedia Eng*. 2015;122:220–7.
11. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in internet of things: the road ahead. *Comput networks*. 2015;76:146–64.
12. Y. Wang and Z. Wu, "Blockchain-based multidimensional trust management in edge computing," *IEEE Access*, 2023.
13. Azzedin F, Ghaleb M. Internet-of-things and information fusion: trust perspective survey. *Sensors*. 2019;19:8.
14. Magruk A. The most important aspects of uncertainty in the internet of things field - context of smart buildings. *Procedia Eng*. 2015;122:220–7.
15. M. Spiliopoulou, M. van Keulen, H.-J. Lenz, J. Wijsen, M. Renz, R. Kruse, and M. Stern, "08421 working group: Imprecision, diversity and uncertainty: Disentangling threads in uncertainty management," in *Uncertainty Management in Information Systems*, ser. Dagstuhl Seminar Proceedings, C. Koch, B. König-Ries, V. Markl, and M. van Keulen, Eds., no. 08421. Dagstuhl, Germany: Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany, 2009. [Online]. Available: <http://drops.dagstuhl.de/opus/volltexte/2009/1937>
16. Der Kiureghian A, Ditlevsen O. Aleatory or epistemic? Does it matter? *Structural Safety*. 2009;31(2):105–12.
17. Yang Y, Perdikaris P. Adversarial uncertainty quantification in physics-informed neural networks. *J Comput Phys*. 2019;394:136–52.
18. L. Smith and Y. Gal, "Understanding measures of uncertainty for adversarial example detection," *arXiv preprint arXiv:1803.08533*, 2018.
19. M. Spiliopoulou, M. Van Keulen, H.-J. Lenz, J. Wijsen, M. Renz, R. Kruse, and M. Stern, "Imprecision, diversity and uncertainty: Disentangling threads in uncertainty management," *Proceedings of Dagstuhl Seminar 08421 on Uncertainty Management in Information Systems*, 2009.
20. Zhao W, Jiang H, Tang K, Pei W, Wu Y, Qayoom A. Knotted-line: a visual explorer for uncertainty in transportation system. *J Comput Lang*. 2019;53:1–8.
21. Sacha D, Senaratne H, Kwon BC, Ellis G, Keim DA. The role of uncertainty, awareness, and trust in visual analytics. *IEEE Trans Visualiz Comput Graph*. 2015;22(1):240–9.
22. M. Ravi, Y. Demazeau, and F. Ramparany, "Managing trust and uncertainty for distributed ai systems," in *Rencontres des Jeunes Chercheurs en Intelligence Artificielle, RJCA'2014*, 2014.
23. Wasserkrug S, Gal A, Etzion O. "A taxonomy and representation of sources of uncertainty in active systems. Cham: Springer; 2006.
24. Bilcke J, Beutels P, Brisson M, Jit M. Accounting for methodological, structural, and parameter uncertainty in decision-analytic models: a practical guide. *Med Dec Making*. 2011;31(4):675–92.
25. A. Kendall and Y. Gal, "What uncertainties do we need in bayesian deep learning for computer vision?" in *Proceedings of the International Conference on Neural Information Processing Systems*, 2017, pp. 5580–5590.
26. Hüllermeier E, Waegeman W. Aleatoric and epistemic uncertainty in machine learning: An introduction to concepts and methods. *Mac Learn*. 2021;110(3):457–506.
27. Y.-C.-T. Hu, B.-H. Kung, D. S. Tan, J.-C. Chen, K.-L. Hua, and W.-H. Cheng, "Naturalistic physical adversarial patch for object detectors," in *Proceedings of the IEEE/CVF International Conference on Computer Vision*, 2021, pp. 7848–7857.
28. C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, and R. Fergus, "Intriguing properties of neural networks," in *Proceedings of the International Conference on Learning Representations*, 2014.
29. Priya S, Uthra RA. "An effective deep learning-based variational autoencoder for zero-day attack detection model. Cham: Springer; 2021.
30. I. Manousakis, I. Goiri, R. Bianchini, S. Rigo, and T. D. Nguyen, "Uncertainty propagation in data processing systems," in *Proceedings of the ACM Symposium on Cloud Computing*, 2018, pp. 95–106.
31. Palani K, Holt E, Smith S, "Invisible and forgotten: Zero-day blooms in the iot," in, *IEEE international conference on pervasive computing and communication workshops (PerCom Workshops)*. IEEE. 2016;2016:1–6.
32. Aydos M, Vural Y, Tekerek A. Assessing risks and threats with layered approach to internet of things security. *Measur Contl*. 2019;52(5–6):338–53.
33. Dileep G. A survey on smart grid technologies and applications. *Renew Energy*. 2020;146:2589–625.
34. F. Khan, M. A. B. Siddiqui, A. U. Rehman, J. Khan, M. T. S. A. Asad, and A. Asad, "Iot based power monitoring system for smart grid applications," in *2020 International Conference on Engineering and Emerging Technologies (ICEET)*. IEEE, 2020, pp. 1–5.
35. Bhuiyan EA, Hossain MZ, Muyeen S, Fahim SR, Sarker SK, Das SK. Towards next generation virtual power plant: Technology review and frameworks. *Renew Sustain Energy Rev*. 2021;150: 111358.
36. Z. Alavikia and M. Shabro, "A comprehensive layered approach for implementing internet of things-enabled smart grid: A survey," *Digital Communications and Networks*, 2022.
37. Pal S, Hitchens M, Rabehaja T, Mukhopadhyay S. Security requirements for the internet of things: a systematic approach. *Sensors*. 2020;20(20):5897.

38. N. Robinson, L. Valeri, J. Cave, T. Starkey, H. Graux, S. Creese, and P. P. Hopkins, "The cloud: understanding the security, privacy and trust challenges," *Privacy and Trust Challenges* (November 30, 2010), 2010.
39. Gunduz MZ, Das R. Cyber-security on smart grid: threats and potential solutions. *Comput Networks*. 2020;169: 107094.
40. O. Aouedi, T.-H. Vu, A. Sacco, D. C. Nguyen, K. Piamrat, G. Marchetto, and Q.-V. Pham, "A survey on intelligent internet of things: applications, security, privacy, and future directions," *IEEE Communications Surveys & Tutorials*, 2024.
41. Nixon P, Wagealla W, English C, Terzis S. Security, privacy, and trust issues in smart environments. *Smart Environments: Technologies, Protocols, and Applications*; 2005.
42. A. Dorri, C. Roulin, R. Jurdak, and S. S. Kanhere, "On the activity privacy of blockchain for iot," in *2019 IEEE 44th Conference on Local Computer Networks (LCN)*. IEEE, 2019, pp. 258–261.
43. Tchernykh A, Schwiegelsohn U, Talbi E-G, Babenko M. Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *J Comput Sci*. 2019;36: 100581.
44. Nicanfar H, Talebifard P, Alasaad A, Leung VC. Enhanced network coding to maintain privacy in smart grid communication. *IEEE Trans Emerg Topics Comput*. 2013;1(2):286–96.
45. F. Siddiqui, S. Zeadally, C. Alcaraz, and S. Galvao, "Smart grid privacy: Issues and solutions," in *2012 21st International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2012, pp. 1–5.
46. Damián-Reyes P, Favela J, Contreras-Castillo J. Uncertainty management in context-aware applications: increasing usability and user trust. *Wireless Personal Commun*. 2011;56(1):37–53.
47. S. Pal, M. Hitchens, and V. Varadharajan, "Towards the design of a trust management framework for the internet of things," in *2019 13th International Conference on Sensing Technology (ICST)*. IEEE, 2019, pp. 1–7.
48. Frederiksen M. Trust in the face of uncertainty: a qualitative study of intersubjective trust and risk. *Int Rev Sociol*. 2014;24(1):130–44.
49. Alassaf N, Gutub A, Parah SA, Al Ghamedi M. Enhancing speed of simon: a light-weight-cryptographic algorithm for iot applications". *Multim Tools Applic*. 2019;78(23):32–633.
50. Khairnar S, Bansod G, Dahiphale V. "A light weight cryptographic solution for 6lowpan protocol stack. Cham: Springer; 2018.
51. Said G, Ghani A, Ullah A, Azeem M, Bilal M, Kwak KS. Light-weight secure aggregated data sharing in iot-enabled wireless sensor networks. *IEEE Access*. 2022;10(33):33–571.
52. Pandey JC, Kalra M. A review of security concerns in smart grid. *Innov Data Commun Technol Applic*. 2022;125:140.
53. F. Ramparany, R. Mondi, and Y. Demazeau, "A semantic approach for managing trust and uncertainty in distributed systems environments," in *2016 21st International Conference on Engineering of Complex Computer Systems (ICECCS)*. IEEE, 2016, pp. 63–70.
54. L. Yang, K. Yu, S. X. Yang, C. Chakraborty, Y. Lu, and T. Guo, "An intelligent trust cloud management method for secure clustering in 5g enabled internet of medical things," *IEEE Transactions on Industrial Informatics*, 2021.
55. M. Sun, M. Li, and R. Gerdes, "A data trust framework for vanets enabling false data detection and secure vehicle tracking," in *2017 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2017, pp. 1–9.
56. Jayasinghe U, Otebolaku A, Um T-W, Lee GM, Data centric trust evaluation and prediction framework for iot. In: ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K). IEEE. 2017;2017:1–7.
57. Gopala Krishnan C, Nishan A, Gomathi S, Aravind Swaminathan G. Energy and trust management framework for manet using clustering algorithm". *Wireless Personal Commun*. 2022;122(2):1267–81.
58. Hossain E, Khan I, Un-Noor F, Sikander SS, Sunny MSH. Application of big data and machine learning in smart grid, and associated security concerns: A review. *ieee Access*. 2019;7:13–960.
59. Cui L, Qu Y, Gao L, Xie G, Yu S. Detecting false data attacks using machine learning techniques in smart grid: A survey. *J Network Comput Applica*. 2020;170: 102808.
60. Yang Y, Li W, Gulliver TA, Li S. Bayesian deep learning-based probabilistic load forecasting in smart grids. *IEEE Transa Indust Inform*. 2019;16(7):4703–13.
61. Selim M, Zhou R, Feng W, Quinsey P. Estimating energy forecasting uncertainty for reliable ai autonomous smart grid design. *Energies*. 2021;14(1):247.
62. Karimipour H, Dehghantanha A, Parizi RM, Choo K-KR, Leung H. A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. *IEEE Access*. 2019;7:80–778.
63. Ozay M, Esnaola I, Vural FTY, Kulkarni SR, Poor HV. Machine learning methods for attack detection in the smart grid. *IEEE Transa Neural Networks Learn Syst*. 2015;27(8):1773–86.
64. Rajasekaran AS, Azees M, Al-Turjman F. A comprehensive survey on blockchain technology. *Sustain Energy Technol Assess*. 2022;52: 102039.
65. Mollah MB, Zhao J, Niyato D, Lam K-Y, Zhang X, Ghias AM, Koh LH, Yang L. Blockchain for future smart grid: a comprehensive survey. *IEEE Inter Things J*. 2020;8(1):18–43.
66. "Brooklyn. bmg. brooklyn energy," <https://www.brooklyn.energy/>, [Online: accessed 24-March-2022].
67. "Electron. electron. lounch and operate distributed energy markets." <https://electron.net/>, [Online: accessed 24-March-2022].
68. Khalid R, Samuel O, Javaid N, Aldegeheishem A, Shafiq M, Alrajeh N. A secure trust method for multi-agent system in smart grids using blockchain. *IEEE Access*. 2021;9:59–848.
69. O. Samuel, N. Javaid, A. Khalid, M. Imrann, and N. Nasser, "A trust management system for multi-agent system in smart grids using blockchain technology," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*. IEEE, 2020, pp. 1–6.
70. Kim H, Laskowski M, A perspective on blockchain smart contracts: Reducing uncertainty and complexity in value exchange. In: *26th International conference on computer communication and networks (ICCCN)*. IEEE. 2017;2017:1–6.
71. Ahmad H, Wang L, Hong H, Li J, Dawood H, Ahmed M, Yang Y. Primitives towards verifiable computation: a survey. *Front Comput Sci*. 2018;12(3):451–78.
72. Monroe F, Wyckoff P, Rubin AD. Distributed execution with remote audit". *Ndss*. 1999;99:3–5.
73. Ramachandran G, Nemeth D, Neville D, Zhelezov D, Yalçın A, Fohrmann O, Krishnamachari B. Whistleblower: Towards a decentralized and open platform for spotting fake news. In: *IEEE International Conference on Blockchain (Blockchain)*. 2020;2020:154–61.

74. A. Laszka, A. Dubey, M. Walker, and D. Schmidt, "Providing privacy, safety, and security in iot-based transactive energy systems using distributed ledgers," in *Proceedings of the Seventh International Conference on the Internet of Things*, 2017, pp. 1–8.
75. Gai K, Wu Y, Zhu L, Xu L, Zhang Y. Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. *IEEE Internet of Things Journal*. 2019;6(5):7992–8004.
76. Guan Z, Si G, Zhang X, Wu L, Guizani N, Du X, Ma Y. Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities. *IEEE Commun Magaz*. 2018;56(7):82–8.
77. Kamal M, Tariq M. Light-weight security and blockchain based provenance for advanced metering infrastructure. *IEEE Access*. 2019;7:87–345.
78. Dorri A, Luo F, Kanhere SS, Jurdak R, Dong ZY. Spb: a secure private blockchain-based solution for distributed energy trading. *IEEE Commun Mag*. 2019;57(7):120–6.
79. Khorasany M, Dorri A, Razzaghi R, Jurdak R. Lightweight blockchain framework for location-aware peer-to-peer energy trading. *Int J Elect Power Energy Syst*. 2021;127: 106610.
80. H. D. Dixit, S. Pendharkar, M. Beadon, C. Mason, T. Chakravarthy, B. Muthiah, and S. Sankar, "Silent data corruptions at scale," arXiv preprint [arXiv:2102.11245](https://arxiv.org/abs/2102.11245), 2021.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.