We present a framework for privacy preservation in an information cloud of IoT devices. We contend that privacy provisioning should be located in the user device and must protect the user, the information and the device from breaches in privacy. We elaborate on how the layered privacy model can ensure such privacy provisioning, and justify the device being the provisioning point instead of the cloud alone. We present the point of view that, due to resource limitations of the IoT devices in general, the privacy preserving measures need to be hard-coded in the device technology. We fall short of suggesting various security controls that can be used for secure communication of private data and focus only on controlling the sharing in an untrusted environment where data is represented as database records with three types of attributes: personally-identifying, quasi-identifying and sensitive attributes. The proposed system empowers the data owner to fully decide and control data sharing at an attribute level.

**Keywords:** Cloud data, Data sharing, Internet of Things (IoT), IoT security, Privacy.

**Introduction**

Ironically, the purpose of WEP (wireline equivalent privacy) in the 1999 Edition of the IEEE 802.11 Standard was privacy provisioning, a concept we are still trying to harness (Solove, 2008). With the cloud technology on full throttle, we need to embrace not just the privacy concept but how can it be provisioned in a mass storage of heterogeneous origin that is sharable privately as well as publicly in the big data. The device limitations in the Internet of Things (IoT) have added a new dimension to the problem (Wang et al., 2018). In this paper, we address some of these privacy issues in IoT with our proposed solution and compare it with some of the state-of-the-art models proposed by other researchers. We start in the next section by describing the nature of cloud computing, the consequent privacy requirements, and the impact of IoT on these requirements. That is Section “Privacy in Cloud”, in which we also discuss why privacy must be provisioned at the device level instead of leaving it to the cloud. In Section “Privacy versus Security in Shared Data System”, we discuss in detail the difference between security and privacy from a conceptual as well as implementation point of view. Sections “Privacy Provisioning - The Proposed System” and “Comparison with Other Proposed Privacy Systems” are the main contributions of this paper in which we define privacy provisioning inclusive of the user, the information, and the device. In Section “Comparison
with Other Proposed Privacy Systems”, we compare our proposed privacy system with the contemporary research and other proposed methods and frameworks. Section “Implementation Considerations” is dedicated to a discussion on the implementation of the proposed privacy system. Finally, in the last section, we present conclusions and further research plan, followed by references.

As for the privacy in the IoT goes, the user perception is highly significant but least studied. The difficulty in studying user expectations is that it is highly subjective and with a large variance. Clustering of scenarios using K-models could provide some logic to favoring certain user groups but need a large set of empirical data for the decisions to be accepted at large (Lee and Kobsa, 2016).

Of Privacy, IoT and Cloud

Before moving on the next sections, we will try to be more specific of our definition and assumptions of the key terms privacy, IoT, and cloud in this subsection.

We assume all information and devices have primary owner(s). As Ahmad et al. (2016) are explaining, there are other types of ownerships, such as secondary and tertiary. Privacy is defined roughly as the ability of the primary owner to amend, destroy, share, un-share or permit further sharing of the information or device (Ahmad et al., 2016).

The IoT is a term emerged because of the ability of a broad range of devices to be on the internet. These devices are hard to classify otherwise as they encompass computers, appliances, daily usage articles, such as glasses, and more, including toilets and whatnots. The Internet Protocol (IP) empowers these devices to be able to share data across billions of devices on the Internet. The IP connectivity is so pervasive that IoT is slowly giving way to a new term IoE (Internet of everything) since we are now thinking of even dresses and shoes that will be connected. However, many of these devices will have a small data footprint. This implies narrow bandwidth, low power and low memory. For the purpose of this paper, we consider devices with such constrained resources of energy, capacity and memory.

The humongous interconnectivity of a sprawling internet is not without its challenges – cybersecurity and privacy beings among the most crucial. An increasing number of data centers are providing a vehicle in which large organizations and occasional users can subscribe to storage and computing services and leave security to the provider. These cloud services, as it turns out, can only provide security on a connection-to-connection basis. There is not much available against malicious attempts of clustering and correlating data to extract privacy related information. For the purpose of this paper, by cloud we mean subscriptions by large and small organizations and individuals for storage and sharing of their or their clients’ private information.
Privacy in Cloud

As Henze et al. (2014) pointed out, cloud computing provides a data integration characteristic that suites IoT well. Same data can be applied for various services instead of replicating it for each, be it health care, finance, public records where allowed, or even social networking. The paper in question makes a good case of empowering the user device with privacy controls by reasoning pervasive health care provision. We concur with the paper position that privacy must be a user-defined measure, but will elaborate more why we believe that it can be hard-coded, at least partially - a position not supported by the concrete work in Henze et al. (2014). The key to privacy is in a disclosure as wanted by the data owner (Ahmad et al., 2016). Once the data leaves user device, the ownership may be shared either via an explicit agreement or due to the mere nature of a device allowed to possess data, such as a router. Meeting user expectations about data disclosure while the data is in a cloud of IoT devices, be it pervasive health care, or a cloud-driven smart neighborhood, is the question addressed in this paper. Figure 1 shows the concept of this portable privacy.

**Figure 1. Portable Privacy Concept**

In this scenario, same privacy measures are with the data whether the data is in the device, in transmission, or in the cloud. This could be the case, for example about a patient's health records for which a hospital has a cloud provider. The HIPPA requirements apply to data in the device, in transit and stored in the cloud (Scheutzow, 2004).

We would like to point out here that not all users are technically savvy and can only specify their privacy needs in general terms, however restrictive they might be. In reference to Figure 1, a user can learn whether a device or an application software (App) provides a required level of privacy by looking at their manuals or asking customer service to provide a written statement about it. However, user may not be able to configure proper security for the data transmission in order to preserve the same privacy while data is in transit. It could be vulnerable simply due to a Wi-Fi glitch or something similar. Also, the main data owner, e.g., patient, may not have any say or knowledge about the privacy preservation in the cloud service. Laws, such as the HIPPA Act may come to
rescue in some instances, but not in all, particularly, in social networks which are the most commonly cloud accessible from IoT devices these days. We contend that not only the best enforcer of privacy is the user, but at least part of privacy provision can be implemented in hardware or firmware. The remaining may depend on a negotiation with the application/party with who the data is shared. The roots of our claim lie in the embedded privacy agreement (EPA) (Navuluri et al., 2016; Aftab and Mukkamala, 2017a; b). We will resort to the proposed framework after clarifying a sensitive issue, that is, the difference between privacy and security in the next section.

Privacy versus Security in a Shared Data System

The Privacy Triangle

If an adversary can read from or write to a user device, the privacy of the device is compromised. If, however, it is only reading then the information has to be disclosed to the adversary to qualify for a "breach". In many cases, such as for wireless devices, data is available to be read but if it is appropriately encrypted, the information may not be revealed. If the adversary can break the confidentiality measure, then the privacy of the information is compromised. In many cases, the information cannot be kept confidential, such as when it is shared for research purpose and becomes part of big data. The main privacy concern in this last case is that there should be no identifying information present or derivable from the shared data. The science of identifying an individual and his/her actions, such as route taken in driving, has matured to the point that we need sophisticated techniques for de-identification (Huang et al., 2017). This is especially significant development because of the opposing requirements for future technologies, such as driver-of the car should be published to manage traffic, and on the other hand it should be kept confidential to protect the individual. Less vehicles, where on the one hand, the route has been shown that one does not need identifying information to identify a person about who the information is (Sweeney, 2002). In a database record a combination of attributes called as the quasi-identifiers (QIs) can be used to derive user identity. Several measures proposed for protecting information owner's identity, such as in Sweeney (2002), Machanavajjhala et al. (2007) and Li et al. (2007), have not been able to fully mask the user identity. Therefore, it is imperative that the user privacy is protected in a privacy provisioning system. In fact, the three types of privacy impact each other as shown in Figure 2.
The *owner* in Figure 2 owns both, the information and the IoT devices. An attack, such as a social engineering attack (someone acting as utility personnel and asking private information via phone) can compromise information and device. *Information* is what should not be disclosed to an adversary as it is correlated with the owner. An attack on information, such as disclosure, can result in divulging the personally identifiable information (PII), putting the life and properties of the owner at risk. The *device* itself processes and stores information. An attack on devices, be it destructive or advanced persistent threat (APT), can compromise not only the information but ultimately the safety of the owner. Therefore, the privacy is not related to one of these three entities, but all the three, as they can be attacked once any one of them is compromised.

In Figure 2, we use the example of a smart meter in an advanced metering infrastructure (AMI), the AMI meter and show how a breach in the meter can result in a breach in information privacy, and a breach in a user privacy and so on. Our privacy model is Figure 2 and now we will discuss how it is different from security.

*Information Security*

Whether the information is in user device, in transit or in a cloud, it can be subject to several types of attacks from an adversary. Figure 3 shows a scenario where security and privacy are depicted in light of Figure 2, the privacy triangle.
The two privacy triangles are the owner and user of information. At these end points, the three vertices of the privacy triangles need to be protected. When in transit, all the three vertices are not necessarily present. For example, if the adversary is collecting signal from the airways, this signal needs to be provided with security measures for integrity (against tampering), confidentiality (against disclosure) and availability. When the information reaches the next devices (be it secondary or tertiary user device, such as destination host or a router, as of Ahmad et al. (2016)), all the three vertices of the privacy triangle need protection. As seen from this figure, privacy is driven by data owner's expectations about its disclosure while security is driven by thwarting adversarial actions. While privacy may be an a priori measure, security could largely be reactive to anomaly detection. That also underlines a problem with security measures in a cloud as the anomaly detection may be harder in a cloud environment (Butun et al., 2015). In fact, in our framework, we assume that security is provided perfectly and address the question of hiding private information while permitting shared information.

Figure 3 uses the AMI meter as an IoT device. It shows that the three types of privacy measures are needed whether the information is in the device, in transit on a network or delivered to a data user. Security measures are needed against hacking attacks for disruption or advanced persistent threat (APT). There is a possibility for jamming, eavesdropping and man-in-the-middle attacks while the data is communicated over a network link. These attacks do not necessarily have to result in a breach in privacy but could simply be for disrupting a service, corrupting information or just to make the information or infrastructure unavailable. If the information can be securely shared between a legitimate owner and users, but can be processed to extract information that was not meant to be shared, such as through inference. This makes the shared information susceptible to attacks on privacy. Security measures could not suffice in providing privacy in this case. For a system to provide privacy, we need to define the goals and then how to achieve these goals. In case of IoT, the privacy goals relate to data at rest as well as in motion (Cisco, 2017). In the
Privacy Provisioning—The Proposed System

The Embedded Privacy Agreement (EPA)

In this sub-section, we briefly describe the EPA. The EPA provides privacy through access control, negotiation and security measures against imperfect trust between a data owner and a data user. The access control is implemented on a Read/Write (R/W) layer where a smallest data unit can be (un)shared using the tuple (R, W), where R, W ∈ (0, 1). A value of 0 arbitrarily denotes a lack of permission for Write (or Read) and a value of 1 vice versa. Thus, a record can be masked at the output of a communication with the help of sequence of (R, W) tuples. This sequence is determined through negotiation, much like a service level agreement (SLA) in quality of service (QoS) provided communications. The propagation of private information is controlled through defining a trust value between the sharing parties and security measures to attain a higher trust level if needed. In a nut shell, EPA defines a privacy filter via negotiation that helps share the negotiated data fields only. The R/W, EPA (negotiation) and trust form the three layers of the privacy provisioning system assumed for this paper. This is shown in Figure 4 (Aftab and Mukkamala, 2017a). In Ahmad and Mukkamala (2017a; 2017b) we have fully described the R/W layer and the EPA layer but not the trust layer. Trust in general is still a work in progress and by looking into the Table 1 of Yan et al. (2014) one can appreciate the fact that the meaning and properties of trust vary from scenario to scenario and application to application. However, no privacy provisioning system will be complete without addressing trust, and therefore it completes in picture for privacy in our view. Interestingly, in Yan et al. (2014), trust management is also in a separate plane that impacts all the IoT layers (see Figure 1 in Yan et al. (2014) for example).

Figure 4. Privacy Provisioning System Using EPA (Aftab and Mukkamala, 2017b)
Limitations of IoT Devices

IoT devices’ capabilities are compared to a client-server architecture. These devices can be dedicated for an ultra-low personal area network (PAN) functioning, such as pedometer displaying information from a step-counting sensor. Out of the six categories of IoT devices in Perera et al. (2014), four have low computational levels (also, see Trappe et al. (2015) for energy constraints). These devices have low power microprocessors with not much memory or bandwidth. Therefore, when we think of a general IoT devices we must assume that it has (i) low processing speed, (ii) low energy/battery, (iii) low bandwidth and (iv) low memory. To provide privacy effectively, part of the privacy protection must be provided in hardware or firmware. Current trends in protecting the cipher keys inside a processor include both software and hardware methods, such as Intel 6+ generation processors, Trusted Platform Module (TPM) (Guan et al., 2015). These measures are against memory disclosure attacks and propose either protecting parts of memory by encrypting the keys or using a separate chip just for security. A similar architecture with added EPA is the proposed framework. In a nut shell, the privacy architecture described more generically in Aftab and Mukkamala (2017a) and Aftab and Mukkamala (2017b) is proposed here as an implementation framework for IoT devices. In Aftab and Mukkamala (2017a), a quantifiable privacy model is proposed, while in Aftab and Mukkamala (2017b) a layered architecture of a network using an embedded privacy agreement (EPA) is described, while here, the proposal is to split the EPA between the device and a privacy server so that device and information owner has some control but privacy server provides additional computing and storage resources.

Hardware-based EPA

For IoT devices, implementation of security in hardware is pretty much a given. Dedicated security co-processors such as proposed in Tsai et al. (2015) can be another hardware-based approach in addition to security and instruction set for security in the main cpu chip of an IoT device. The EPA consists of two parts, a global part and a local part (Ahmad and Mukkamala, 2017a; 2017b). The global EPA sets the baseline for privacy and the local EPA is based on the negotiation and can vary from data user to data user. Figure 5 shows the difference between the two using a database record as an example.

**Figure 5. Red Fields Make a Global EPA and Black Ones, One or More Local EPA**

| Record ID | Name      | Age | SSN       | Race     |
|-----------|-----------|-----|-----------|----------|
| 100100    | Michael Joe | 38  | 123-45-6789 | Caucasian |
| Permissions | (Read, Write) | (Read, Write) | (Read, Write) | (Read, Write) |
In Figure 5, there are four attributes, Name, Age, SSN and Race. The red attributes are disclosed under no circumstances, thus making the global EPA, while the others can be disclosed depending on the local EPAs negotiated. In the proposed model, the global EPA is set up one time in the firmware while the local EPA is configurable for each sharing instance. The global EPA is inside the hardware device and user controlled even if the device is owned by a provider, such as a utility company depending on smart grid communications with a smart meter.

It is prudent to mention here that we are not proposing a significant rethinking of the hardware design. Embedded security solutions are easily and cheaply available in many forms, such as Trusted Platform Module, TrustZone, Intel's and AMD new secure chip architectures, such as Security Extension Guards (SGX). Ukil et al. (2011) discuss some of these available options. We are proposing to do a similar thing for privacy.

**Comparison with other Proposed Privacy Systems**

Several researchers proposed various privacy models in the context of IoT. In this section, we will discuss some of the proposed models and how our model compares with those existing models. Some of the proposed models are hardware based and some are software based.

Maycock and Sethumadhavan (2016) proposed a hardware enforced privacy mechanism. They proposed including a new hardware chip called privacy protection unit, that sits between the IoT sensors and the data processors to broker the sensitive information while preserving privacy. They suggest that the hardware could also be a programmable unit, which we believe will be vulnerable to tampering. Also, different users of these IoT devices have different data needs and a single policy on the hardware alone will not be sufficient to provide adequate privacy to the information.

Babar et al. (2011) proposed a security framework for IoT, in which they suggest using a hybrid approach where the hardware and software are both involved in providing the security for the information. They suggested to use cryptographic algorithms to protect the information and the proposed architecture also involves several complex hardware functional units to be added to the hardware to protect the keys for cryptographic algorithms and for other secure storage. Several IoT devices that are used are commonly are dumb devices which do not have much storage or computational capability, which is why they have become so inexpensive. Our approach involves minimal hardware changes and addition to the firmware of the device, which is a one-time investment and very inexpensive.

Henze et al. (2014) presented a user-driven privacy enforcement for cloud based services in IoT. Their approach is perhaps the closest to our proposed solution. They introduced Privacy Enforcement Points (PEP) that sit on the network gateways to enforce the privacy requirements, outside the user’s private network. They suggest that the user’s privacy configuration is stored on
the PEP and that the user will have an interface to use their interface to read the generated privacy policy. EPA in our proposed architecture is similar to the concept of PEP, but it actually is not static and is encapsulated with the data and travels with the information on the network. Our EPA’s exist both on the IoT device and on the software, that is interfacing the IoT device, thus providing a standard privacy agreement at the global level where the sensitive information can be identified and completely hidden from the software and the software level local EPA provides a second layer of privacy by enabling more granular privacy configuration.

Though there are several approaches, of which some are software based, some are hardware based and some are hybrid approaches, our proposed approach provides a more granular privacy control to the user. One big advantage of the approach is that the EPA can be applied and enforced even when the data leaves the user’s network, because the EPA is also very extendable and it can dictate which user can access which parts of the information. Most approaches do not consider the case where the user must give write access to parts of the information. The proposed approach can provide the user to dictate such agreements in EPA to control access to the information. The owner also may have to allow the users to share certain information, which access can be controlled with the EPA. Once the data leaves the owner’s network and the access is provided to a user, the user does not have a control on how the information is used or shared. The EPA will help the owner to protect their information by giving them the control to decide if the information they are providing the user can be shared.

This shows that the architecture is very robust and extendable. The global and local EPA’s provide the owner the maximum control over how and what parts of the information is accessed or shared.

**Implementation Considerations**

The proposed privacy provisioning system can be implemented in many ways. To make it flexible enough to give the user ability to dictate his or her privacy baseline, a user configurable ROM like implementation at the time initial hardware set up may be the most suitable. Accordingly, when a user uses the device the very first time, a ‘global EPA’ is accompanied with the information entered. Following table shows a sample Global EPA for the AMI meter.
Table 1. Sample Global EPA for a Smart Meter

| Attribute        | Value                  | Read | Write | Expiry |
|------------------|------------------------|------|-------|--------|
| Prefix           | Mr.                    | Y    | N     | Never  |
| First name       | Michael                | Y    | N     | Never  |
| Middle name      | John                   | Y    | N     | Never  |
| Last name        | Doe                    | Y    | N     | Never  |
| SSN              | 123-45-6789            | Y    | N     | Never  |
| Driver's License | VA-XYZ                 | Y    | N     | Never  |
| Phone number     | (xyz)abc-defg          | Y    | Y     | Never  |
| Primary care phone | (123)456-789       | Y    | N     | Never  |
| Primary email address | mjdoe@doe.name    | Y    | Y     |        |
| Suffix           | II                     | Y    | N     | Never  |
| Prefix           | Ms.                    | Y    | N     | Never  |
| First name       | Michele                | Y    | N     | Never  |
| Middle name      | Jay                    | Y    | N     | Never  |
| Last name        | Doe                    | Y    | N     | Never  |
| SSN              | 101-11-2131            | Y    | N     | Never  |
| Suffix           |                        | N    | N     | Never  |
| Driver's License | VA-XYZ                 | Y    | N     | Never  |
| Phone number     | (xyz)abc-defg          | Y    | Y     | Never  |
| Primary care phone | (123)456-789       | Y    | N     | Never  |
| Primary email address | mjdoe@doe.name    | Y    | Y     |        |
| Address          | San Francisco          | Y    | Y     | Never  |
| Address type     | Residential            | Y    | N     | Never  |
| Active alarm     | Fire                   | Y    | N     |        |
| Meter ID         | ABC123                 | Y    | N     | Never  |

As seen from Table 1, all attributes are sharable at this level, some are both readable and writeable (phone and email).

Now consider a local EPA with a fire alarm company that uses the same meter as a communication medium. The local EPA can consist of the Table 2.
Table 2. Local EPA with a Fire Alarm Company

| Attribute           | Value          | Read | Write | Expiry |
|---------------------|----------------|------|-------|--------|
| Prefix              | Mr.            | Y    | N     | Never  |
| First name          | Michael        | Y    | N     | Never  |
| Middle name         | John           | Y    | N     | Never  |
| Last name           | Doe            | Y    | N     | Never  |
| SSN                 | 123-45-6789    | N    | N     | Never  |
| Driver's License    | VA-XYZ         | N    | N     | Never  |
| Phone number        | (xyz)abc-defg  | Y    | Y     | Never  |
| Primary care phone  | (123)456-789   | N    | N     | Never  |
| Primary email address| mjdoe@doe.name| Y    | Y     |        |
| Suffix              | II             | Y    | N     | Never  |
| Prefix              | Ms.            | Y    | N     | Never  |
| First name          | Michele        | Y    | N     | Never  |
| Middle name         | Jay            | Y    | N     | Never  |
| Last name           | Doe            | Y    | N     | Never  |
| SSN                 | 101-11-2131    | N    | N     | Never  |
| Suffix              | N              | N    | N     | Never  |
| Driver's License    | VA-XYZ         | N    | N     | Never  |
| Phone number        | (xyz)abc-defg  | Y    | Y     | Never  |
| Primary care phone  | (123)456-789   | N    | N     | Never  |
| Primary email address| mjdoe@doe.name| Y    | Y     |        |
| Address             | San Francisco  | Y    | N     | Never  |
| Address type        | Residential    | Y    | N     | Never  |
| Active alarm        | Fire           | Y    | Y     |        |
| Meter ID            | ABC123         | Y    | N     | Never  |

As seen from Table 2, some fields, such as SSN, Driver's License, Primary care's phone number, are not shared. On the other hand, the Fire alarm can be read and written (for resetting, e.g.) by the alarm company/fire department, depending on who the agreement is with. The smart meter example is very important because of the expectation that it will convert future homes into smart homes and will do many things done by different systems today, such as caring for the elderly, controlling humidity in the backyard, turning on/off appliances, ordering everyday items directly by looking at the refrigerators,
ordering medicines automatically, and providing the News updates on the owner's topic of interest (Weiss et al., 2012). The above example clearly illustrates how the hardware component can provide a baseline privacy and local EPAs can provide the overlay agreements instead of sending all the information all the time. Figure 6 shows how is this possible in an IoT cloud.

For more details on how negotiation for Global and Local EPA are implemented, the reader is referred to Ahmad and Mukkamala (2017a; 2017b). As we mention in the next section, the proposed system is close to the one in Henze et al. (2014). If we compare Figure 1 with Figure 6, we can see the similarities of general scenarios. The gateways (GW) in Figure 1 would be replaced by cloud or data warehouse server and is not shown in Figure 6 for simplicity sake (Navuluri et al., 2016; Ahmad and Mukkamala, 2017a; b). The user-authorized services in Figure 1 is provided via the Local EPA in Figure 6. The main difference between the two papers is obvious from Figure 2 and Figure 6 in this paper. From Figure 2, we see that the privacy enforcement point (PEP) is in user-control, which we assume is best implemented in hardware. However, the privacy policy (PP) in Figure 2 is in the cloud entirely. While one may argue that the PEP will protect the data that is not sharable, the metadata about this data still may be shared. Also, in our proposal, one may block some user attributes entirely and forever. For example, if user has his/her medical results in a folder in AMI meter, these results can optionally be blocked forever from transmitting to the IoT cloud so the PP and PEP in this way are both enforced in the user device. The default policy in Henze et al. (2014) is a close relative of Global EPA in this paper with the difference that EPA provides access control to each attribute of each data record. To differentiate between security and privacy, our proposed method does not propose the use of individual encryption keys for each attribute but negotiate the sharing extent. We leave the actual security of the information and device as an open issue to be decided by the data owner, data user and cloud service provider. Figure 3 makes this clear. Using EPA, only that data flows through the channel between a data owner and a data user that has been agreed upon under the negotiated EPA. Securing that data is a different issue.

**Figure 6. Multifarious Use of Smart Meter under EPA**
Conclusions and Future Course

In this paper, we lay the foundation of understanding and providing privacy in a cloud of the Internet of Things (IoT). Given the limited nature of resources available for such devices and complex nature of the privacy provisioning, we propose that part of the provisioning system should be within the device and part negotiated with the sharing application. We propose the use of an elaborate privacy system consisting of three layers to provide an attribute by attribute negotiated privacy agreement in an untrusted network and show how parts of a data record can be shared on an as needed basis. We plan to continue work reported here and set up a laboratory environment for testing the proposed system. Privacy has been defined as consisting of inability of disclosure of the user, the information and the device. The privacy provisioning problem is defined as how the data sharing can take place as specified by the data owner without any breach in any of the three scopes of the privacy, the user identity disclosure, the unwanted information disclosure, and the unwanted device access.

Acknowledgments

The authors are indebted to the anonymous reviewers for valuable suggestion to enhance the readability of the original manuscript and for clarifying certain points.

References

Ahmad, A., Misra, P., Ono, F., Priest, C., Suarez, J. and Urcioli, A. (2016). The information privacy domain. *International Journal of Information Privacy, Security and Integrity*, 2(4), 307-329.

Ahmad, A. and Mukkamala, R., "On Information Privacy Metrics". *14th International Conference on Information Technologies: New Generation (ITNG) 2017*, Nevada Las Vegas, April 2017a.

Ahmad, A. and Mukkamala, R., "A Novel Information Privacy Model: A Layered Approach", *14th International Conference on Information Technologies: New Generation (ITNG) 2017*, Nevada Las Vegas, April 2017b.

Babar, S., Stango, A., Prasad, N., Sen, J. and Prasad, R. (2011). Proposed embedded security framework for internet of things (iot). In *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)*, pp. 1-5.

Butun, I., Kantarci, B. and Erol-Kantarci, M. (2015). Anomaly detection and privacy preservation in cloud-centric Internet of Things. In *Communication Workshop (ICCW)*, pp. 2610-2615.

Cisco (2017). The Internet of Things Reference Model. Available at https://bit.ly/1vEwE7W.

Guan, L., Lin, J., Luo, B., Jing, J., & Wang, J. (2015, May). Protecting private keys against memory disclosure attacks using hardware transactional memory. In *Security and Privacy (SP), 2015 IEEE Symposium on* (pp. 3-19). IEEE.
Henze, M., Hermerschmidt, L., Kerpen, D., Häußling, R., Rumpe, B. and Wehrle, K. (2014). User-driven privacy enforcement for cloud-based services in the internet of things. In Future Internet of Things and Cloud (FiCloud), pp. 191-196.

Huang, Y., Li, S. C., Tai, B. C. and Chang, C. M. (2017). De-identification Technique for IoT Wireless Sensor Network Privacy Protection. Jurnal Ilmu Komputer dan Informasi 10 (1), 1-10.

Lee, H. and Kobza, A. (2016). Understanding User Privacy in Internet of Things Environments. Internet of Things (WF-IoT).

Li, N., Li, T. and Venkatasubramanian, S. (2007). t-closeness: Privacy beyond k-anonymity and l-diversity. In Data Engineering, pp. 106-115.

Machanavajjhala, A., Kifer, D., Gehrke, J. and Venkitasubramaniam, M. (2007). l-diversity: Privacy beyond k-anonymity. ACM Transactions on Knowledge Discovery from Data (TKDD) 1 (1), 3.

Maycock, M. and Sethumadhavan, S. (2016). Hardware Enforced Statistical Privacy. IEEE Computer Architecture Letters 15 (1), 21-24.

Navuluri, K., Mukkamala, R. and Ahmad, A. (2016). Privacy-Aware Big Data Warehouse Architecture. In Big Data (BigData Congress), pp. 341-344.

Perera, C., Jayaraman, P. P., Zaslavsky, A., Georgakopoulos, D. and Christen, P. (2014). Mosden: An internet of things middleware for resource constrained mobile devices. In System Sciences (HICSS), pp. 1053-1062.

Scheutzow, S. (2004). HIPAA: A Primer. GPSolo 21, 39.

Solove, D. (2008). Understanding privacy. Available on the Internet via google scholar.

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10 (05), 557-570.

Trappe, W., Howard, R. and Moore, R. S. (2015). Low-energy security: Limits and opportunities in the internet of things. IEEE Security & Privacy 13 (1), 14-21.

Tsai, C. R., Hsiao, M. C., Shen, W. C., Wu, A. Y. A. and Cheng, C. M. (2015, May). A 1.96 mm 2 low-latency multi-mode crypto-coprocessor for PKC-based IoT security protocols. In Circuits and Systems (ISCAS), pp. 834-837.

Ukil, A., Sen, J. and Koilakonda, S. (2011). Embedded security for Internet of Things. In Emerging Trends and Applications in Computer Science (NCETACS), pp. 1-6.

Wang, H., Zhang, Z. and Taleb, T. (2018). Special issue on security and privacy of IoT. World Wide Web 21 (1), 1-6.

Weiss, M., Helfenstein, A., Mattern, F. and Staake, T. (2012). Leveraging smart meter data to recognize home appliances. In Pervasive Computing and Communications (PerCom), pp. 190-197.

Yan, Z., Zhang, P. and Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. Journal of network and computer applications 42, 120-134.
