International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 9, No.3 (May-2020)
http://dx.doi.org/10.12785/ijcds/090306

Privacy Concerns In IoT
A Deeper Insight into Privacy Concerns in IoT Based Healthcare

Mohamed Sarrab [1] and Fatma Alshohoumi [1]

[1] *Communication and Information Research Center, Sultan Qaboos University, Al- Khoudh, Oman*

Received 2 Jan. 2020, Revised 19 Feb. 2020, Accepted 13 Apr. 2020, Published 1 May 2020

Abstract: IoT technology provides great solutions in many fields including healthcare, military, logistics, etc. It aims to collect data and process it to provide useful services and knowledge. However, a tradeoff exists between collecting data and providing services wherein the service providers have to deal with the data of individuals to deliver tailored services and the individuals have concerns about their privacy. Revealing of user's information leads to a compromise in user privacy. IoT devices leak sensitive information prone to misuse. This study conducts a deeper investigation into IoT data privacy. It discusses the IoT privacy concerns in healthcare and provides a complete scenario of the IoT data flow with privacy concerns. Moreover, the paper thoroughly discusses privacy in the IoT data flow in IoT-based healthcare and suggests privacy solutions in each phase. The paper's outcomes showed that privacy in the IoT occurs at different stages of the IoT data flow. It also showed that the types of privacy concerns and the mitigation mechanisms differ at each phase of IoT data. Future research will extend this work to design privacy preservation mechanisms that suit the nature of IoT-based healthcare.

Keywords: IoT, Internet of things, IoT Privacy Concerns, Private Information, Data Mining, Privacy Preservation Techniques, IoT-Based Healthcare.

1. INTRODUCTION

Presently, the world is entering the fourth industrial revolution, which plays a role in changing the way we live and work. The fourth industrial revolution will shape the future through its great impacts on government and business [1]. Internet information technologies such as the Internet of things, big data, artificial intelligence, cloud computing, nanotechnologies, biotechnologies, and other advanced technologies have penetrated each other, thus bringing about the fourth industrial revolution [2]. The technology of the Internet of Things (IoT) is a recent communication paradigm that invades our daily life with many applications that make our lives easier, safe, and smart [3]–[5]. Many definitions for IoT have been derived by scholars; however, still, it does not have a standard definition [6]–[10]. The essence of IoT is that all things surrounding us can connect to the internet and exchange data anywhere and at any time [11]–[13]. IoT achieves its goal of facilitating the interaction between things by relying on other supporting technologies such as fog computing, big data, cloud computing, wireless sensor network, distributed computing, nanotechnology, wireless communications, etc. [3], [14]–[17]. The IoT technology intervenes in many domains of daily life, such as automobiles, transportations, education, healthcare, environment, energy management, elderly assistance, industry, etc. [11], [13], [18]–[21] [22]. Technology reports on IoT have shown a dramatic change in the way we work and live due to the impact of IoT on the industry and society [5]. The potential economic impact of IoT and its supporting technologies are estimated to go from $3.9 trillion to $11.1 trillion by 2025 [23]. It provides great benefits such as home monitoring, health monitoring, agriculture monitoring, energy monitoring and control, environmental monitoring, smart education, smart security, etc. [24], [25]. Regardless of the great benefits offered by IoT, many challenges and concerns hinder the development and the success of the promising technology of IoT [26]–[28]. Many surveys such as [26]-[27], [29]–[35] were conducted to discuss the challenges of IoT. Nevertheless, to date, security and privacy concerns are the major challenges [36]–[38] that scholars continue to discuss and address. Security issues and solutions to mitigate them were discussed by many researches such as in [8], [39]–[46], etc. As the core of IoT is the collection of data, the pervasive nature of IoT imposes many threats to an individual's privacy [47]. Thus, the confidence about privacy is considered the driving factor for IoT's success [48]. Recently, scholars have been focusing on user privacy in IoT and have started taking the privacy issues in IoT into account, according to [22], [49]–[58]. Little work has been done to protect sensitive sensors data after the data is collected and stored [59]. Therefore, there is an inevitable need to address the privacy issues in IoT architecture and propose a privacy-preservation framework for IoT. This work sheds light on investigating IoT data privacy in general and IoT-based healthcare data flow with privacy

E-mail: sarrab@squ.edu.om, alshohoumi@squ.edu.om

concerns in particular. To the best of our knowledge, this is the first work that takes a closer

look at data flow (phases) in IoT-based healthcare and thoroughly discusses the privacy concerns in each data phase.

The remaining paper is organized as follows: Section 2 presents the methodology that has been followed to achieve the work of this research. Section 3 introduces background knowledge and related work, including a brief background on the evolution of IoT and IoT architecture. Section 4 introduces the privacy concept. Section 5 conducts an in-depth investigation into the privacy in IoT and discusses it from different angles (during life, at the end of life), thoroughly discusses privacy in the IoT dataflow, and reviews the privacy threats in IoT. Section 6 and section provide deeper insights into the privacy concerns in IoT-based healthcare.

Section 8 provides an analysis of the data collection of eight IoT-based medical devices and suggests solutions to mitigate user privacy concerns based on other disciplines similar to IoT, such as data mining and data publishing. In section 9, the conclusion is drawn along with the research question for future research.

2. RESEARCH METHODOLOGY

To accomplish the aim of the conducted paper, Figure 1 illustrates the research methodology that has been used to achieve the specified research objectives.

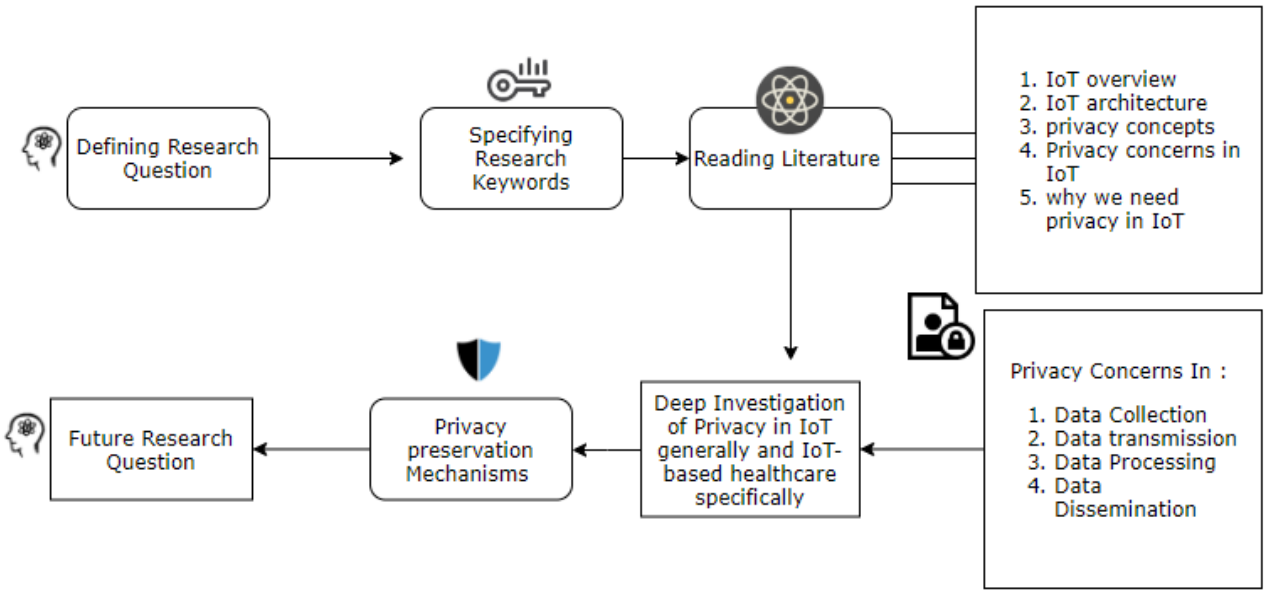

Figure. 1. Methodology of the Research

As shown in Figure 1, the methodology includes six phases, described as follows:

1. First phase: defining the research questions.

The main research questions of this paper are:

- What are the privacy concerns in IoT data and how can we avoid privacy concerns in IoT? This question is divided into sub-questions, as follows:
  - What is the privacy concept?
  - What is the rationale behind privacy preservation in IoT?
  - Where do privacy concerns occur (at which phase of the IoT data flow)?
  - Do privacy preservation mechanisms exist?

2. Second phase: choosing research keywords.

The research keywords used for the search were ‘internet of things’, ‘IoT’, and combinations of terms including: ‘privacy’, ‘privacy concerns’, ‘data collection privacy’, ‘data processing privacy’, ‘data dissemination privacy’, ‘data transmission privacy’, ‘privacy protection’, ‘private information’, ‘privacy preservations’, ‘data mining privacy’, and ‘data publishing privacy preservation’.

3. Third phase: Literature. In this phase, many databases such as google scholar, scoups, research gate, IEEE Internet Comput, IEEE Trans, ICACTE, IEEE Wirel. Commun., Futur. Gener. Comput. Syst, IGI Global, EEE Commun, IEEE Int. Conf. Consum., J. Healthc. Eng, Int. J. Inf. Technol, ICCCN, etc., were searched. Many papers were used to answer research questions and assemble a background on IoT, IoT architecture, privacy concept, privacy concerns in IoT, and the rationale behind IoT privacy preservation.

4. Fourth phase: a deeper insight into IoT privacy. In this phase, attention was focused on analyzing the privacy concerns in the IoT data flow.
5. Fifth phase: a deeper insight into privacy in an IoT-based healthcare system. In this phase, the academic search was restricted to studying the privacy concerns at each phase in IoT-based healthcare systems.
6. Sixth phase: Future research questions were specified.

As shown in Figure 1, the methodology includes six phases, described as follows:

7. First phase: defining the research questions.

The main research questions of this paper are:

- What are the privacy concerns in IoT data and how can we avoid privacy concerns in IoT? This question is divided into sub-questions, as follows:
  - What is the privacy concept?
  - What is the rationale behind privacy preservation in IoT?
  - Where do privacy concerns occur (at which phase of the IoT data flow)?
  - Do privacy preservation mechanisms exist?

8. Second phase: choosing research keywords.

The research keywords used for the search were 'internet of things', 'IoT', and combinations of terms including: 'privacy', 'privacy concerns', 'data collection privacy', 'data processing privacy', 'data dissemination privacy', 'data transmission privacy', 'privacy protection', 'private information', 'privacy preservations', 'data mining privacy', and 'data publishing privacy preservation'.

9. Third phase: Literature. In this phase, many databases such as google scholar, scoups, research gate, IEEE Internet Comput, IEEE Trans, ICACTE, IEEE Wirel. Commun., Futur. Gener. Comput. Syst, IGI Global, EEE Commun, IEEE Int. Conf. Consum., J. Healthc. Eng, Int. J. Inf. Technol, ICCCN, etc., were searched. Many papers were used to answer research questions and assemble a background on IoT, IoT architecture, privacy concept, privacy concerns in IoT, and the rationale behind IoT privacy preservation.
10. Fourth phase: a deeper insight into IoT privacy. In this phase, attention was focused on analyzing the privacy concerns in the IoT data flow.
11. Fifth phase: a deeper insight into privacy in an IoT-based healthcare system. In this phase, the academic search was restricted to studying the privacy concerns at each phase in IoT-based healthcare systems.
12. Sixth phase: Future research questions were specified.

3. Background Knowledge

Presently, the world is going into the fourth industrial revolution, which, in addition to relying on the internet on a large scale, is introducing advanced technologies such as IoT. The term IoT started gaining popularity in academia and industry in 1999 when it was coined by Kevin Ashton. The executive director of the Auto-ID Center at Massachusetts Institute of Technology [7], [19], [60], [61] [20]. Generally speaking, the evolution of advanced technologies such as RFID, wireless sensor networks, cloud computing, IPV6, nanotechnologies, etc. were the major trends behind the emergence of IoT [19] [62]. RFID, which is used for identifying things with tags, was used extensively in 2003 and 2004 [19]. In 2009, however, the number of devices connected to the internet exceeded the number of people and statistics showed that the expected number of connected IoT devices will reach 30.73 billion devices by 2020 and 75.44 billion by 2025 [63]-[64]. IoT's fundamental objective is to make things connect to the internet and thus facilitate interaction with things [53]. As a result, IoT offered great opportunities in critical domains such as location-based services, smart homes, smart cities, e-health [65], [66], E-learning [67], E-business [68]-[69], environment, transportations, etc. [9] [70] [26].

Consequently, different IoT architectures were devised. In 2008, the first IoT architecture was introduced by Pereira to describe the layers that IoT is composed of [62], [71]. However, this architecture didn't give IoT a comprehensive meaning. In 2010, Tan in [62] improved the previous IoT architecture by adding a new layer that added further details of the IoT architecture. As shown in Figure 2, in the same year, the 3-layer architecture of IoT, consisting of the perception layer, network layer, and application layer, was proposed by Miao et al. in [10]. It simply described IoT and its layers as follows: the perception layer contains all devices used for sensing and collecting data from the surrounding environment such as RFID, 2-D barcode, and even nanotechnologies. The network layer is the core of IoT used for transferring the collected data to the layer above (the application layer) through communication media such as Wi-Fi, Bluetooth, ZigBee, etc. The top layer was the application layer, which is basically used for managing IoT applications.

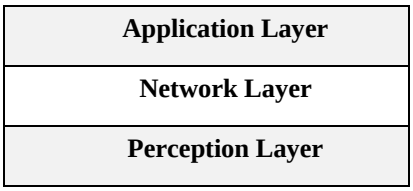

Figure 2. The Three Layers of the IoT Architecture

This architecture was considered as the accepted IoT architecture. Nonetheless, it still did not provide a comprehensive meaning for IoT. Following this, another IoT architecture was proposed in 2010 to improve the 3-layer architecture by adding two extra layers. This architecture composed of 5 layers as shown in Figure 3. It

introduced the processing layer used for storing, analyzing, and processing the information received from the network layer. The business layer was introduced to consume the data obtained from the application layer to build business models, graphs, and flowcharts, which are useful for evaluating the new technology of IoT. This architecture provided a basic understanding of IoT in which it covered the idea of IoT and summarized it briefly as collecting data using IoT devices, transmitting the data over the internet for storage and processing, and followed by extracting and presenting the knowledge obtained from the collected data.

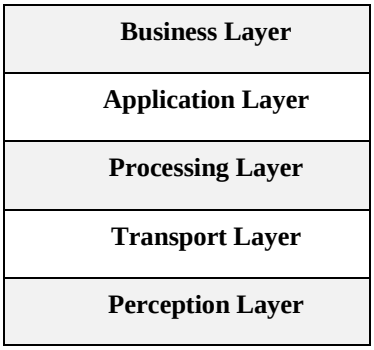

Figure 3. Five-Layer IoT Architecture

In 2010, the development of IoT was in its initial stage. Many challenges stand as obstacles that impact the sustainability of IoT, such as scalability issues, data volumes, data interpretation, interoperability, fault tolerance, power supply, wireless communication, privacy, security, etc., as mentioned in the surveys in [26]-[27], [29]–[35]. IoT architectures that were proposed after 2010 addressed these challenges as proposed in [7], [27], [44], [72]–[75], [76]. So far, there is no standard IoT architecture[53][77]. To date, security and privacy are considered as the topmost challenges that need to be addressed, and these are considered a complementary requirement for IoT [36]–[38][78]. This research focuses on generally investigating the privacy issues in IoT and specifically investigating IoT-based healthcare.

4. Privacy Concept

Some researchers consider privacy as part of security issues [53] [79] [43]. Indeed, there is a noticeable difference between the terms of privacy and security [80]. The term security deals with securing the privacy of data, data through communication, data at storage, data at processing, and securing the access of data [43] [81], while the term privacy belongs to persons and their data, especially the data with a high degree of sensitivity [53]. Precisely, every person should have the right to control his private data [82]. The term information privacy or data privacy became popular from the 1960s due to the rise of electronic data processing [83].In 1890, Warren and Brandeis in their article 'The Right to privacy' defined privacy as "the right to be let alone" [84]. Following this, Westin defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" in his book Privacy and Freedom [85]. He described it as the right that everyone possesses to control the personal information gathered about them [85]. He also said that with respect to their privacy, people can be classified into three groups: Fundamentalist, Pragmatist, and Unconcerned [86]. Fundamentalists are a group of people who are concerned about the accuracy of the collected data and the uses of the data. Fundamentalists support laws and privacy rights, while Pragmatists are willing to provide their personal information to trusted parties in order to use their services. However, the Unconcerned group consists of those who fully trust that third parties who collect their personal data will not abuse it [87]. Westin's follow up surveys showed that the number of concerned people had declined in the last few years in which people start taking care of their privacy [86]. Other definitions of privacy are provided by scholars. For example, Gavison said, "A loss of privacy occurs as others obtain information about an individual, pay attention to him, or gain access to him". Barth said, "Privacy is the right to appropriate flows of personal information". Additionally, according to Bertino, he defined privacy as "The right of an entity to be secure from unauthorized disclosure of sensitive information that is contained in an electronic repository or that can be derived as aggregate and complex information from data stored in an electronic repository" [88]. Therefore, privacy can be summarized as the release of information in a controlled way.

Although IoT has the potential to change our way of dealing with the things around us, it is exposed to momentous security and privacy risks [89]. Privacy involves the concealment of personal information and the ability to control personal data [90]. More specifically, privacy determines that a person has the right to decide the level of his interaction with the environment or the amount of his data that can be viewed by the public [53] [91] [82]. Weak security measures in IoT devices lead to privacy breaches and safety threats in the real world [92]. There are large overlaps and intersections between security and privacy concepts, but there is a notable difference between them. Generally, the manufacturers of IoT have concentrated and have been taking care of hardware security more than caring about user's privacy[53] [93] [94]. However, privacy deals with certain aspects such as those depicted in Figure 4 [53].

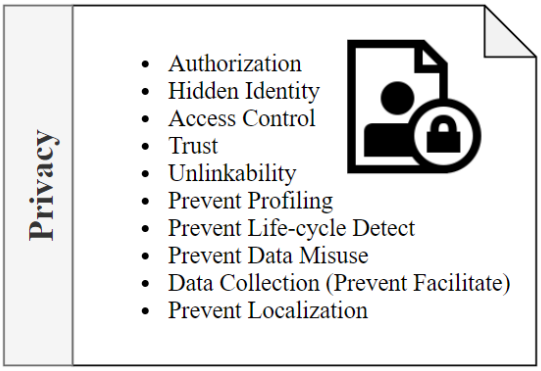

Figure 4. Privacy Aspects.

Privacy has been classified into four components by privacy internationals [87] as depicted in Figure 5. The first component is body privacy that is related to people's physical protection against exterior harm. The second

component is communication privacy, which focuses on protecting information carried through media such as networks, mobile phones, etc. The third component is the territory privacy that protects the physical space, public places, home, property, etc. The fourth component is information privacy that is referred to as personal data that is collected, stored, and processed by an organization [95]. The next section focuses more on information privacy in IoT.

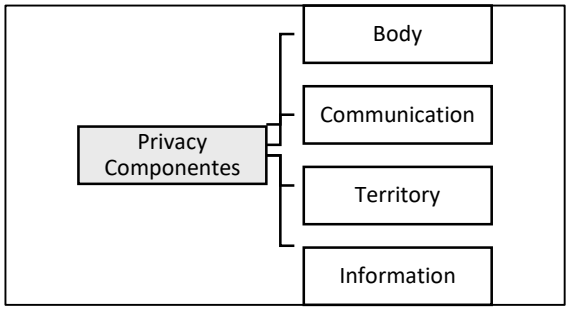

Figure 5. Privacy Components

5. PRIVACY IN IOT

In IoT, devices use sensors to collect data from the surrounding environment and then transfer them over the internet to cloud servers that store, process, and learn from the data. This nature of data collection, transmission, and optimization exposed to serious privacy concerns. In particular, IoT devices that collect data can incidentally reveal sensitive data. Moreover, the collected data can be sent to an untrusted local network or untrusted third party without users' control [22]. Indeed, IoT users tend to believe that they own the data produced by IoT devices and don't have a clear knowledge of how the collected data is used by cloud services or which data are may reveal [22]. Moreover, recent studies have shown that IoT devices can leak sensitive information [22]. For example, the data collected by smart switches, smart thermostats, and smart power meters can leak information such as whether or not a home is occupied [96]–[98]. Furthermore, IoT devices such as rooftop solar panels can reveal home location [99]-[100]. In solar energy analytics, energy data can leak location information, which can cause location-based privacy attacks [22].

In a critical field such as the military, the privacy threat is very dangerous as IoT devices can leak sensitive information that the enemy can exploit. For instance, the Strava fitness app posted a map of its users' activity on the internet. Security researchers showed that this public activity map imposed a severe threat on the U.S national security by indirectly revealing the locations and behaviors or attitudes of U.S military bases and personnel in Syria and Iraq [22] [101].

In the smart car, vulnerabilities that can threaten life have been found. Tesla Model S was hacked by the security researchers at Keen Security Lab in the form of disrupting all the features of the car such as brakes, door lock, disclosure of their locations, and controlling the computer, from a distance of 12 miles [102].

In 2014, HP Security Research conducted an analysis of 10 of the most popular IoT devices on the market in order to investigate their security and privacy issues [102] [103]. They found that 90% of these devices collected information and transferred it over the cloud without requiring a complex password. They also found that 70% of these devices allow the attackers to identify user accounts through enumeration. Moreover, their analysis showed that 6 out of 10 of these devices did not use encrypted network services. These findings indicate that the privacy of users can be compromised.

A. *Privacy Threat*

The following Figure 6 summarizes the privacy threat to IoT data:

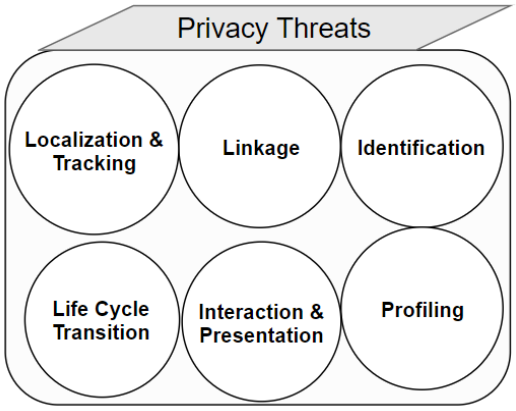

Figure 6. Summary of Privacy Threats

As shown in Figure 6, the identification of things owners have connected to the internet can pose privacy threats as the identifier may involve sensitive details such as IDs, names, etc. Localization and tracking through GPS by IoT devices can reveal details of owners' locations that cause a serious privacy threat. Some of these applications, such as apps related to e-commerce use profiling for personalization, through which the organization can mine the collected data of individuals to infer their interest, leading to privacy threats. Smart things can interact with systems and give feedback to users. This interaction leads to privacy threats in which private or sensitive data can be revealed and violated. Life cycle transitions of such smart IoT things can threaten the privacy of its owner. Even if the owner assumes that all information is deleted, the smart device can store a huge amount of data and their own history during their entire life cycle. Linkage of different IoT systems can pose privacy threats since there is a chance of unauthorized access and leaks of private information [87] [70].

B. *Rationales the Need for Privacy Preservation in IoT*

Although IoT provides great solutions to humanity, the invisibility of the data collection, usage, sharing of data, and presentation of data raise many privacy concerns. The privacy of users could be easily lost [87] [104]. Taking privacy in IoT into account leads to a wider acceptance of IoT by customers, in turn leading to IoT success [89]. In 2013, a survey conducted by the IEEE internet of things showed that 46% of respondents consider privacy concerns

as the biggest obstacle to IoT adoption. The large scale of data collection by IoT devices poses significant privacy challenges that may impede the development of IoT [83]. Indeed, service providers have to access and deal with users' information for the purpose of providing or delivering tailored services [87]. However, users expect their private information to be protected from illegal access and not exposed to third parties [105]. Therefore, users have to obey the service provider by providing their information in order to utilize the provided services. The service providers have to preserve users' privacy to help IoT succeed in the market. This trade-off should be solved to utilize IoT's benefits while achieving users' satisfaction on the one hand and IoT sustainability on the other.

In IoT, privacy preservation can be achieved through two approaches, as illustrated in Figure 7.

The first approach is privacy by policy approach. In this approach, the privacy policy should be implemented in the data collection phase. Actually, the privacy policies are designed to provide answers to questions such as: "by whom is the information collected?", "What kind of information is collected", "why and how is the information collected, used, and protected?", "Is information being shared with anyone?" etc. [106]. In most cases, as discussed by Schaub and his colleagues in [107] [106], privacy policies are ineffective due to some reasons. For example, the complexity of notice texts, in which the terms are mostly long and include complicated texts. Moreover, the lack of choices leads to a misunderstanding about data practices. Additionally, the time of viewing these policies is inappropriate as the user sees the notice only during the installation time. As the IoT devices' screens are very small, it is impossible to view their privacy policies [106].

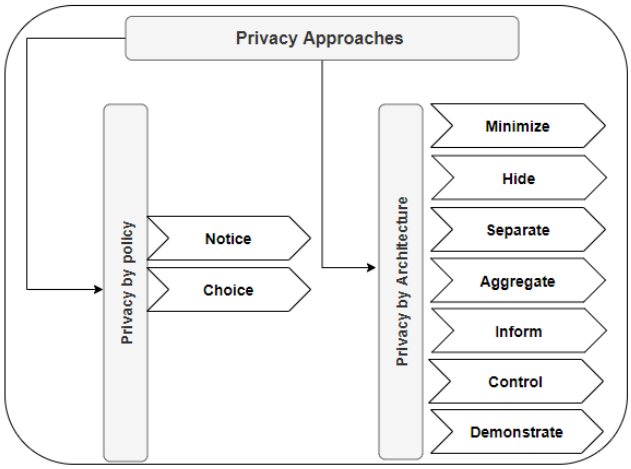

Figure 7. Privacy Approaches

The second approach, which is the privacy by architecture, involves the eight privacy design strategies that are categorized into data-oriented strategies, such as (minimize, hide, separate, and aggregate), and process-oriented strategies, such as (inform, control, enforce, and demonstrate) [83].

- Minimize strategy involves minimizing the collection the personal information.
- Hide strategy means that personal information and its interrelationships should be hidden to avoid any unintended use.
- Separate means that personal information should be separated and processed in a distributed fashion.
- Aggregate strategy means that the information should be processed at the highest level of aggregation.
- Inform strategy means that the individuals should be informed whenever their information is collected and processed.
- Control strategy means that individuals should be provided agency over the processing of their personal data.
- Enforce strategy refers to a privacy policy compatible with legal requirements.
- Demonstrate signifies being able to demonstrate compliance with the privacy policy and any applicable legal requirements.

As discussed earlier, different concerns may occur during different IoT phases. Therefore, in each phase, the data privacy can be preserved using a data protection mechanism that will be suited to the nature of data in each phase.

C. *A Deeper Insight into Privacy in IoT Phases*

Despite the type of IoT applications, privacy breaches can occur in IoT during the life cycle of IoT devices and at the end of their life, as depicted in Figure 8.

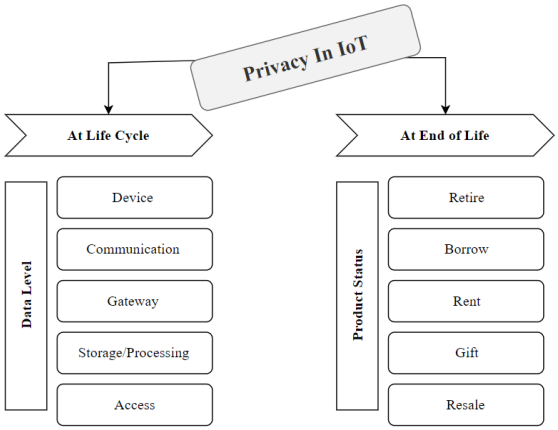

Figure 8. Privacy in IoT

During the life cycle of IoT, privacy can be violated in different IoT data flows, such as at the data collection phase, data transmission, data processing and storing, and at data dissemination and reporting. While, at the end of life of IoT devices, privacy can be invaded during the rent, retire, borrow, gift, and resale acts actions.

D. *Privacy Concerns at End of IoT Life:*

As seen in Figure 8, privacy concerns may occur during the life cycle of an IoT device or at the end of its life. The Figure presents five acts that the consumer may do without

any awareness of privacy concerns. In the first act, the consumer can borrow the IoT device of some other person. A potential privacy breach may occur this way because the IoT product that has been borrowed is configured to the owner's credentials. Additionally, this IoT device may be connected to the owner's devices and, thus, his data is exposed to privacy issues [54]. In the act of renting the IoT device, a number of privacy issues can arise. For example, if the IoT smart home devices are rented, these devices may help unauthorized persons exploit vulnerabilities that can facilitate serious privacy risks. When the owner of the IoT devices gives his device as a gift to another person, privacy issues can arise since the second person has to use the device that contains the personal information of its first owner [54]. The same case will happen when the IoT device is resold. When the IoT device is retired, if not properly disposed of, it will cause serious privacy issues [54].

E. Privacy Concerns at IoT Lifecycle

During the life cycle of IoT, privacy concerns occur in all IoT data phases. In IoT, the data can go through four main stages starting with data collection, followed by data transmission and data processing and ending with data dissemination. Data collection is performed by IoT devices, in which the data from the surrounding environment is sensed. Four aspects of the information domain can be collected by IoT devices [108]. The first aspect is the identification information, which is specific to the owner of the IoT device, such as username, address, phone, credit card number. The second aspect is the environmental data, and this differs according to the purpose of the data collection. It involves data related to health statuses such as temperature, insulin level, heart rate, etc., and data related to weather status such as humidity, CO2 concentration, rain level, etc. The third aspect is related to the IoT device data such as device identifier (IP address, MAC address, Network information, etc.). The fourth aspect is related to the location information that will help identify a user's location. Therefore, the persuasive nature of data collection by IoT can lead to serious privacy issues related to a revelation of sensitive information related to the user's activities [109]–[112]. After the data has been collected, it will be transmitted through communication media such as Wi-Fi, Bluetooth, etc. For processing purposes, during the transmission, the sensitive data can be exposed to serious attacks, which leads to a breach of privacy [112]. The transmitted data can be modified and revealed by a man-in-the-middle attack, thus compromising the privacy of an individual. In the processing phase, the collected data can be stored in different places such as in the gateway, central-local servers, distributed servers (fog computing), and cloud services. Sensitive data stored in these solutions (server, Fog, and cloud computing) are exposed to attacks and privacy threats. Persistent storage such as cloud servers can raise significant privacy concerns while transient storage such as gateway has minimal privacy implications [112]. The collected data can be sold to third parties without the user's consent, which actually leads to a compromise of privacy.

F.Privacy Solutions at IoT Lifecycle

To avoid privacy issues during the data collection phase, the industries of IoT devices should follow the privacy policy principles identified in [113]. There are 11 fundamental privacy principals [55], described as follows:

1. Notice/awareness: This policy states that the privacy policy statement should be clear and explicit.
2. Data Minimization: This policy means that the evaluation of the necessity of the collected data should be conducted before deployment.
3. Purpose specification: Here, the purpose of data collection should be specified.
4. Collection limitation: This policy means that the IoT device should carefully collect necessary data only.
5. Use limitation: Personal data should not be disseminated for an unintended purpose.
6. Onward transfer: This policy means that the collected data should not be transferred to third parties if they do not ensure adequate protection.
7. Choice/consent: This policy says that users should be able to make a decision on the collection, use, and disclosure of their private and personal information. In other words, a mechanism for opt-in and opt-out should exist.
8. Access/participation: This policy says that an individual should be able to access their stored data.
9. Integrity/accuracy: Here, the data controller should ensure the accuracy of the collected data and it should be up to date.
10. Security: According to this, the collected data should be secured from external attacks.
11. Enforcement: This policy mandates the inclusion of a mechanism to enforce privacy principals.

In the second phase, the data is transmitted through communication media. In this phase, the data should be concealed from any expected attack that may, later on, break the privacy of users by disclosing the sensitive data and using it for unintended purposes. Mechanisms to secure the data through transmission include encryption techniques such as homographic cryptography. It is well known that encryption techniques require more computations and powers especially when the data is large. In IoT, the devices are resource-constrained. Therefore, lightweight encryption mechanisms are needed to protect the collected data during the transmission phase. During the processing phase, the data is stored and computed. The data can be stored centrally in local servers, sent to distributed servers near IoT devices, or it can be sent to the cloud solutions. Many privacy concerns, such as user profile, localization tracking, and information linkage, can rise in this phase. During data processing, the collected data can be integrated from different sources. This integration of data leads to information linkage in which the information belonging to different services can be correlated, which can reveal insights about users and their locations [114]. Data anonymization mechanisms are

needed to provide privacy protections for the stored data. User privacy can be compromised when the data is shared with third parties without the user's consent. The shared data can be used for unknown purposes or in an improper way. Figure 9 depicts the privacy scenario across the IoT lifecycle.

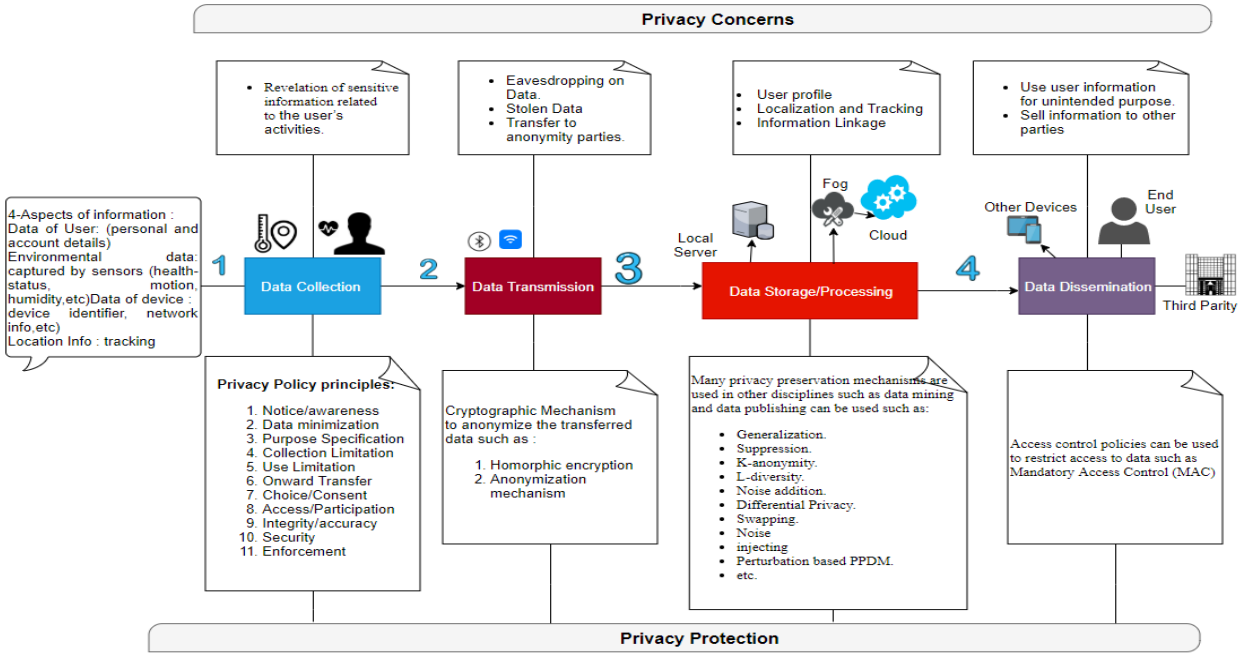

Figure 9. The Complete Scenario of Privacy Concerns in IoT Data Flow.

6. Privacy Concerns in IoT-Based Healthcare System.

Before Nowadays, due to the pivotal role of healthcare in ensuring good care for an individual in any country, huge resources and investments are being poured into healthcare to provide better services for individuals. Unfortunately, many factors, such as the increasing aging populations and the rise in chronic diseases, cause significant strain on modern healthcare systems [115]. Thus, the demand for resources such as hospital beds, doctors, and nurses are extremely high [116]. For example, statistics from China, show that the aged population has exceeded 200 million and is rising by 8 million a year [117]. In America, the statistics expected that by 2020, the number of people who need assistance will reach 117 million, and yet the total number of unpaid caregivers such as family members is expected to reach only 45 million [118], [119]. This increase in the age population that needs assistance causes several problems such as regular treatment, demand for extra resources, rehabilitation, etc. Obviously, there is a need for a solution in order to decrease the pressure on healthcare systems and at the same time continue to provide high-quality care [115]. Healthcare forms the most attractive application area for IoT [120]. The Forbes magazine report suggests that the market for IoT in healthcare will reach 117$ billion by 2020 [118].

IoT has been widely used and deployed in healthcare. For example, some hospitals have started implementing smart beds that can detect whether the beds are occupied or whether the patients are attempting to get up and sending these notifications or information to caregivers.

Moreover, these beds can be adjusted to ensure the appropriate pressure without caregiver intervention [118].

IoT-based systems can be used for tracking changes in patients with progressive conditions such as Parkinson's disease by tracking and recording its symptoms such as slowed movement, gait problems, tremors, and balance problems [123]. Through the use of wearable accelerometers, these symptoms can be measured and learned using machine learning algorithms in order to identify the rate at which the patient's symptoms are deteriorating. Critical health can be monitored using various wearable sensors that sense vital and other important signs including body temperature, blood pressure, pulse, and respiratory rate. Sensors sense these vitals regularly to notify patients and healthcare providers whether any of these vitals are falling below a known healthy threshold in order to get better diagnoses accordingly.

Although IoT helps in enhancing the quality of life, managing real-time diseases, and increasing user experience [124], IoT applications are exposed to attacks and vulnerabilities [125]. In IoT devices such as the insulin pumps that were manufactured by Medtronic company, the systems of these devices do not provide adequate security to the command sent to the pump by patients. This lack of security leads to serious privacy issues such as a revelation of the patients' information to third parties, interception and alteration of commands, and even threatening of a patient's life by the administration of a fatal insulin dose to the patient [102].

Wearable health trackers have mostly used IoT devices nowadays. Fitness trackers track the location of users explicitly, thereby leaking and revealing the user's sensitive information and location [22]. Researchers conducted a deeper investigation into these systems and found that these systems are targeted by men during middle attacks, resulting in a disclosure of their wearers' sensitive information [102] [126]. For example, IoT devices such as wearable fit trackers and health bands are used for monitoring activities such as running, walking, sleeping, heart rate, skin temperature, etc. Moreover, the locations where these activities are performed are recorded by these devices. Wearers of these devices can share information about these activities using social media. The sharing of health data leads to privacy implications such as a revelation of details about the wearers' health [22]. For example, the Apple Watch collects the heart rate data of their wearers, and the researchers found that the mining of such data can detect abnormal or irregular heart rates and atrial fibrillation (AFIB) that causes stroke [127]. Though this detection is beneficial for users of these devices, their private and health data can be revealed by third parties and is prone to misuse [22].

IoT devices collect patients' information for further processing and computation to provide quality services. Privacy concerns remain a crucial aspect of healthcare. Patients expect that their identifiable information will remain secret and confidential. The IoT-based healthcare system has guaranteed privacy, yet allows information sharing for the purpose of providing high-quality care [118]. Thus, the protection of privacy in IoT-based healthcare will impact the overall acceptance of IoT by healthcare providers. Thus, more attention should be focused on covering privacy issues across the IoT-based healthcare lifecycle.

7. A Deeper Insight into IoT-Based Healthcare Data Privacy

IoT-based devices collect sensitive data from healthcare in general and patients in particular, such as a patient's bio-signals in order to assist healthcare givers while monitoring the patient's health and enhancing the accuracy of data collection and the quicken the diagnosing process. Thus, different sensors are used for collecting healthcare data such as:

A. Wearable Healthcare Sensors (WBANS)

Various wearable sensors can be used to collect biosignals, location, and activity status from the patients such as:

- Pulse Sensors: It has been widely used for medical purposes and for fitness. Sensing the pulse is crucial to detect risky and emergency conditions such as cardiac arrest, pulmonary embolisms, and vasovagal syncope [115].
- Respiratory Rate Sensors: This sensor is used to measure the number of breaths a patient takes every minute. This measurement is pivotal for detecting conditions such as asthma attacks, hyperventilation, apnea episodes, lung cancer, obstructions of the airway, tuberculosis, etc. [115].
- Body Temperature Sensors: It is very important to sense body temperature to detect health conditions such as hypothermia, heatstroke, fevers, etc. [115].
- Blood Pressure: It is not a vital sign, but it can be measured using three vital signs. It is used to measure hypertension, which causes a heart attack [115].
- Glucose Level Monitoring: It can be used to measure the sugar in the blood. Tracking glucose levels can help in the planning of meals, activities, and medication times for diabetics [125].

B. Special-Purpose Wearable Sensors

These sensors can be used to monitor a specific condition such as:

- Evaluating heart health with Echocardiograms (ECGS). ECGs can also be used to monitor brain activity in order to detect seizures, sleep disorders, and progress after a head injury [115].
- Fall Detection is used to monitor elderly people. To detect falls, a wearable camera can be affixed [128]. Moreover, an accelerometer, a gyroscope, and a magnetometer can be used to accurately detect falls [129].

C. Contextual Sensors

- These sensors are used to monitor room conditions in which the patients stay, such as light conditions, air quality in the room, etc.

The diverse and unstructured patient's health data that are collected by different sensors are sent to cloud servers through communication media for storage and processing, following which, it can be utilized by different intended users. Therefore, the data in IoT-based healthcare go through four phases:

1. Data Sensing: Various medical sensors are used to collect data from patients and the healthcare environment.
2. Data Transmission: The collected data will be transmitted through communication media such as short-range communication standards including Bluetooth Low Energy (BLE) and ZigBee and long-range, which includes Low-Power Wide-Area Networks (LPWANS) such as Sigfox, LORAWAN, and NB-IoT [115]
3. Data Processing and Storage: The collected raw data of healthcare are processed using analytic tools such as machine learning tools. The processing of healthcare data can be executed in the gateway, fog computing, and cloud computing. Due to the huge data collected by IoT medical devices, cloud computing is used for data management, data storage, etc.
4. Data Dissemination: The processed data (reports) can be accessed by the intended users in healthcare.

In healthcare, the patients' data such as identity, location, and bio-signals have a high degree of sensitivity

that touches the patient's privacy. Despite this, IoT offers great solutions in healthcare; the streamed data by IoT-based medical devices are exposed to violations and threats, which can cause serious risks to a patient's life. Data privacy can be breached in different IoT phases as follows:

A. Privacy Violation in the Sensing Phase

The personal data of patients are collected without a guarantee from IoT device providers to preserve the privacy of the patient's data. Data collection principles such as data minimization, etc. as discussed in section 7 must be applied and agreed between suppliers and consumers. IoT devices collect data from patients without getting patients' consent [118] [130]. In order for IoT-based healthcare systems to ensure privacy, the patients have to know what data is being collected, when the data is collected, why it is collected, where the collected data is going, and who owns it. To help reduce privacy risk during the data collection phase, the previously specified 11 fundamental privacy principals in [55] should be used in IoT-based healthcare. The following table presents a description of how the 11 fundamental privacy principals can be used in data collection by IoT-based healthcare:

TABLE 1. USE OF THE 11 FUNDAMENTAL PRIVACY PRINCIPLES IN THE DATA COLLECTION OF IOT-BASED HEALTHCARE

Privacy principles	**Description of the principle in IoT-based healthcare**
Notice/Awareness	Service providers should set a clear privacy policy statement. They should provide enough details about their data collection practices and the privacy policy should be written in a well-organized way with clear language.
Data Minimization	Service providers should evaluate the necessary data for collection before IoT-based healthcare deployment.
Purpose specification	The purpose specification of data collection should be clear.
Collection limitation	IoT-based healthcare systems should collect only the necessary data.
Use limitation	Collected personal information of patients should not be disseminated for an unspecified purpose.
Onward transfer	Collected data of patients should not be transferred to third parties without permission from healthcare.
Choice/Consent	Patients and healthcare users should be able to decide on the collection, use, and disclosure of their personal data.
Access/participation	Patients should be able to access their data.
Integrity/accuracy	IoT-based healthcare system controller should ensure the accuracy of the collected data, and it should be up to date.
Security	The collected data should be secured from external attacks.
Enforcement	The policy should include a mechanism to enforce privacy principals.

B. Privacy Violation in the Data Transmission Phase

Like any other system connected to the network, during data transmission, the transmitted data is exposed to privacy issues such as data manipulation, which leads to the destruction of patients' privacy, severely affecting the patient's life. For example, if a vital sign such as heart rate is modified by a man-in-the-middle, this will be a threat to the patient's life after the diagnosis. In order to prevent such a scenario, the transmitted data should be protected using an encryption mechanism such as a homographic encryption scheme. The Symmetric key cryptography algorithms, which are an advanced encryption standard (AES) can be used because they are used for large data and are suitable in healthcare, where the data stored in cloud servers; it also requires a low RAM for processing and has high speed [131]. In 2019, Janakiraman and his colleague used a lightweight watermarking algorithm for IoT application to secure medical information and the images of patients' by inserting patient's identities as an invisible watermark in random edge pixels of images [132]. Perturbative techniques such as noise injecting were used to avoid the disclosure of values of a sensitive attribute in data mining [133]. Noise injecting meant that a value obtained from probability distribution will be added to the personal information or sensitive attributes. This method can help data during transmission because even if data is intercepted by the-man-in-the-middle, it remains ambiguous and thus the patient's privacy is preserved.

C. Privacy Violation in Processing and Storage Phase

Due to the large volume of data, which are collected by sensors, it is necessary, to extend the cloud in order to solve issues related to computation, networking, and storage. Thus, the fog is a new paradigm for distributed computing. It helps to reduce the volume of data and traffic to the cloud, improve latency and quality of service. It provides useful services for IoT applications in healthcare. However, it is exposed to security and privacy issues like a cloud [134]. Security and privacy mechanisms can be employed in fog but the research on this area is still in the early stage [134].

Data stored in the cloud are exposed to serious privacy attacks. For example, stakeholders exploit a patient's data to offer them useful services without a guarantee of privacy preservation. Privacy preservation for data in the cloud can be achieved through encryption mechanisms. Additionally, the data can be split into many servers in the cloud and that will help in further preservation of users' privacy because even if one server gets compromised, users' confidentiality can still be preserved [59]. Many privacy preservation mechanisms are used in other disciplines such as data mining and data publishing, which have the same nature of IoT of data collection and data processing. Appendix 1 provides a description of some of the existing data preservation techniques. Furthermore, machine learning and deep learning can be used for protecting the stored data and thus preserving the privacy of patients[135]–[137].

D. Privacy Violation in Data Dissemination Phase

Stored data in the cloud can be disclosed by unintended users and can be utilized for unknown purposes. Thus, it leads to a compromise in the patient's privacy. The stored data in the cloud can be accessed only by intended users by employing access control policies. Mandatory Access Control (MAC) mechanism, which is a rule-based system, can be used for restricting access to data. Moreover, the recent access control mechanism is called cipher-text

attribute-based encryption (CP-ABE) which potentially ensures data security and privacy in smart health[138].

8. DISCUSSION

Section 7 provides details about data privacy in IoT healthcare by thoroughly discussing each phase of the IoT system in healthcare. To the best of our knowledge, this is the first work that takes a closer look at data flow (phases) in IoT-based healthcare. To support the discussion in this work and to explore the data collection practices of these IoT-based medical devices, eight of IoT-based medical devices were investigated. Up-to-date privacy policies of IoT-based medical devices were downloaded for the analysis. Table 2 presents the analysis of the eight IoT-based medical devices, the actual medical data collected by them, and the criticality level of the collected data. Besides, the security guarantee statement provided in their privacy policies were presented

TABLE 2. EIGHT IOT-BASED MEDICAL DEVICES ANALYSIS IN TERMS OF THE COLLECTED DATA AND THE PROVIDED SECURITY STATEMENT.

Healthcare IoT app	Collected Medial Data	Criticality level	Security Guarantee Statement
InPen[139]	Insulin doses such as amounts, date and time of each injection, and information and analyses derived from such data.	High sensitive	"No data transmission or storage system can be guaranteed to be 100% secure".
Vista Solution™ platform[140]	Measure eight vital sings: Single-lead ECG, heart rate, heart rate variability, respiratory rate, body temperature, body posture, fall detection, activity, blood pressure, weight, oxygen saturation.	High sensitive	"Since no method of the trans internet or electronic storage is 100% secure, we cannot guarantee its absolute security".
Withings Sleep[141]	Measure physical activities such as number of steps, distance traveled, number of swimming stroke, number of calories burned, type of activity, level of activity, and sport session time. Body metrics data such as (weight, muscle, fat, water percentage, heart rate, blood pressure, electrocardiogram, heart sound, temperature, sleep cycles, snoring episodes.	High sensitive	-
The Dexcom G5® Mobile CGM System[142]	Measures glucose readings, date, and time.	High Sensitive	-
OneTouch Ping®[143]	Measures blood glucose readings.	High Sensitive	"Unfortunately, no data transmission over the Internet or data storage system can be guaranteed to be 100% secure".
Kardia[144]	Collects raw electrocardiogram ("ECG," "EKG") measurement data, average heart rate, and location on the body where the ECG recording was taken (e.g., body or chest).	High Sensitive	"No data security measures can guarantee security. We are not responsible for any lost, stolen, or compromised passwords or for any activity on your account via unauthorized password activity".
Mynotifi(automatic fall detection)[145]	Measures fall and location of fall.	High sensitive	-
Qardio[146]	Records ECG data, heart rate, heart rate variability, skin temperature, respiratory rate, and activity tracking.	High Sensitive	"Given the nature of communications and information processing technology, Qardio cannot guarantee that Information, during transmission through the Internet or while stored on our systems or otherwise in our care, will be safe from intrusion by others".
Zio TX[147]	Measure the patient's heart rhythm.	High Sensitive	"No security system is impenetrable, and we cannot guarantee the security of the website, nor can we guarantee that the information you supply will not be intercepted while being transmitted to us over the internet, and we are not liable for the illegal acts of third parties".

Table 2 shows that IoT-based medical devices collect various medical data for diagnosing several diseases such as heart disease, diabetes, etc. Different measurements can be taken such as heartbeats, skin temperature, blood pressure, respiratory rate, etc. These measurements vary in the criticality or sensitivity level in which some measurements especially those belonging to the heart may affect patients' life if deliberate or unintentional faults or misuse of data occur. For example, in 2015, the security researcher Billy Rios demonstrated that he could remotely control the patients' insulin pump and administer a fatal dose of drugs through it. Recently, Johnson & Johnson informed patients who have the Animas OneTouch Ping medical device that the system is vulnerable because data during the communication phase are not encrypted. The hacker can gain access to the device and enforce it to deliver a lethal dose of insulin to diabetic patients[148]. As presented in Table 2, the security guarantee statement provided in the privacy policies of these devices is negative in which it provides no warranty on securing the personal information of users who use these apps. Indeed, with no guarantee of securing personal data, the customer would not trust such apps.

TABLE 3. ANALYSIS OF PRIVACY RISKS IN EACH PHASE IN IOT-BASED HEALTHCARE WITH SUGGESTIONS FOR PROTECTION TECHNIQUES

IoT phase	Data Type_ status/ Privacy risk	Risk status/justification	What type of data preservation needed?	How	Privacy Approach	Suggestions
Data Sensing	Raw data Unprotected devices lead to more occurrences of data breaches and increased risks to patients' safety.	High In which personal data such as identification and location can be revealed.	Privacy policy principles that are discussed in 8.	Study whether these principles are used for medical devices or not If we enforce all these principles for IoT medical devices, can we preserve privacy?	Privacy by policy	Enforce the use of data protection principles to help reduce privacy risk at data sensing phase
Data Transmission	Unhidden raw data is exposed to various attacks such as man-in-the-middle attack during transmission	High In which patients data can be altered, which can lead to patients' deaths during treatment due to altered data, especially in high-risk cases	Data can be hidden through data encryption mechanisms	There exist several data encryption algorithms, such as advanced encryption standards.	Privacy by Architecture	IoT medical devices continuously send the sensed data; the suggested encryption algorithm should be light because IoT devices are resource-constrained. And there is no need for all streamed data to be encrypted
Data Processing (Fog)	hidden processed patients' data can harm patients' privacy	High In which any leak of processed data can expose patient data to privacy violations	Data filtering and data protection is needed	Data protection algorithms in gateway should consider resources available in the gateway.	Privacy by Architecture	Many privacy preservation mechanisms are used in other disciplines such as data mining and data publishing, which have the same nature of IoT of data collection and data processing. Appendix 1 provides a description of some of the existing data preservation techniques
Data Storage (Cloud)	Storing data in one place with plain text and without awareness of who can reach the data and use it will violate patients privacy	Extremely high In which patients' data can be accessed by unintended users and used by third parties.	To preserve patients' privacy, the stored data can be distributed to many cloud servers with the encrypted format, so the policy agreement between healthcare and service providers should be clear	Data distribution mechanisms with data protection should be used Clear policy agreement between service providers of cloud and healthcare	Both Privacy by Architecture & privacy by policy	

Data Access	Getting patients' data stored in the cloud without policy restrictions can cause serious privacy violations	High In which data will be revealed and used for illegal purposes	A policy for restricting access to data should be used	Access control policies should be used by healthcare to manage and control all access to the patient's data.	Privacy by policy	Mandatory Access Control (MAC) mechanism that is a rule-based system will be used for restricting access to data. This mechanism is used in a high-security.

Each phase in IoT-based healthcare is exposed to privacy violations that require a solution to mitigate such violations. In the data collection phase, a set of data collection principles must be employed and agreed between the device provider and consumer. For example, the collected data must be minimized to just the data necessary for the required service. Moreover, the data collection policy should be clear to patients themselves in order to gain their trust and know what happens with their private data. During the data transmission phase, the collected data needs to be hidden from any attack as the transmitted data goes through the network. Any modification to the collected data may cause harm to the patients' life and even their death. The violation also should be mitigated after the data have been processed in the fog and stored in the cloud, which can be vulnerable to any kind of attack that destroys the privacy of the patients' information. The restrictions for accessing stored data by intended users should be placed carefully by employing access control policies. Based on the above analysis, the overall scenario of dataflow in IoT-based healthcare and the required privacy solutions in each phase can be illustrated as Figure 10 shows:

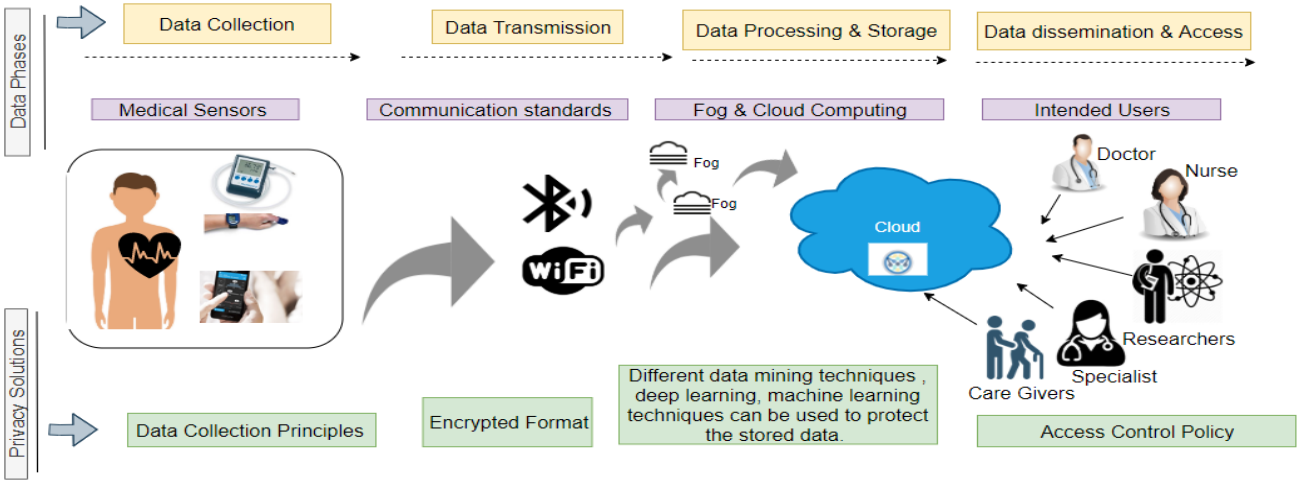

Figure 10. Scenario of Dataflow in IoT-Based Healthcare and the Required Privacy Solutions at Each Phase.

In brief, data generated by IoT-based medical devices move through the main four phases, as shown in Figure 10, starting with the data collection phase which includes several IoT-based medical sensors (devices) used for collecting biosignals from patients. The data generated by these sensors vary in the type of data, the purpose of collection, and the criticality level of the collected data. The raw collected data need further processing and thus the collected data move through the transmission phase over communication standards to the next phase for computation and storage whether to nearby servers (fog) or to the cloud servers. The last phase of the collected data is the dissemination phase in which the collected data are accessed for diagnosing and decision making. Data breaches may occur in any phase and result in affecting the integrity of data, the release of patients' information which indeed leads to cause severe harm to patients' privacy. Hence, different privacy preservation mechanisms can be employed in each phase to preserve the privacy of data. This works provides a deep insight into data privacy in IoT-based healthcare through investigating the data privacy in each phase of data and suggests privacy preservation mechanisms that can be employed in each phase. The graphical summary of the whole taxonomy discussed in this work is presented in Figure 11.

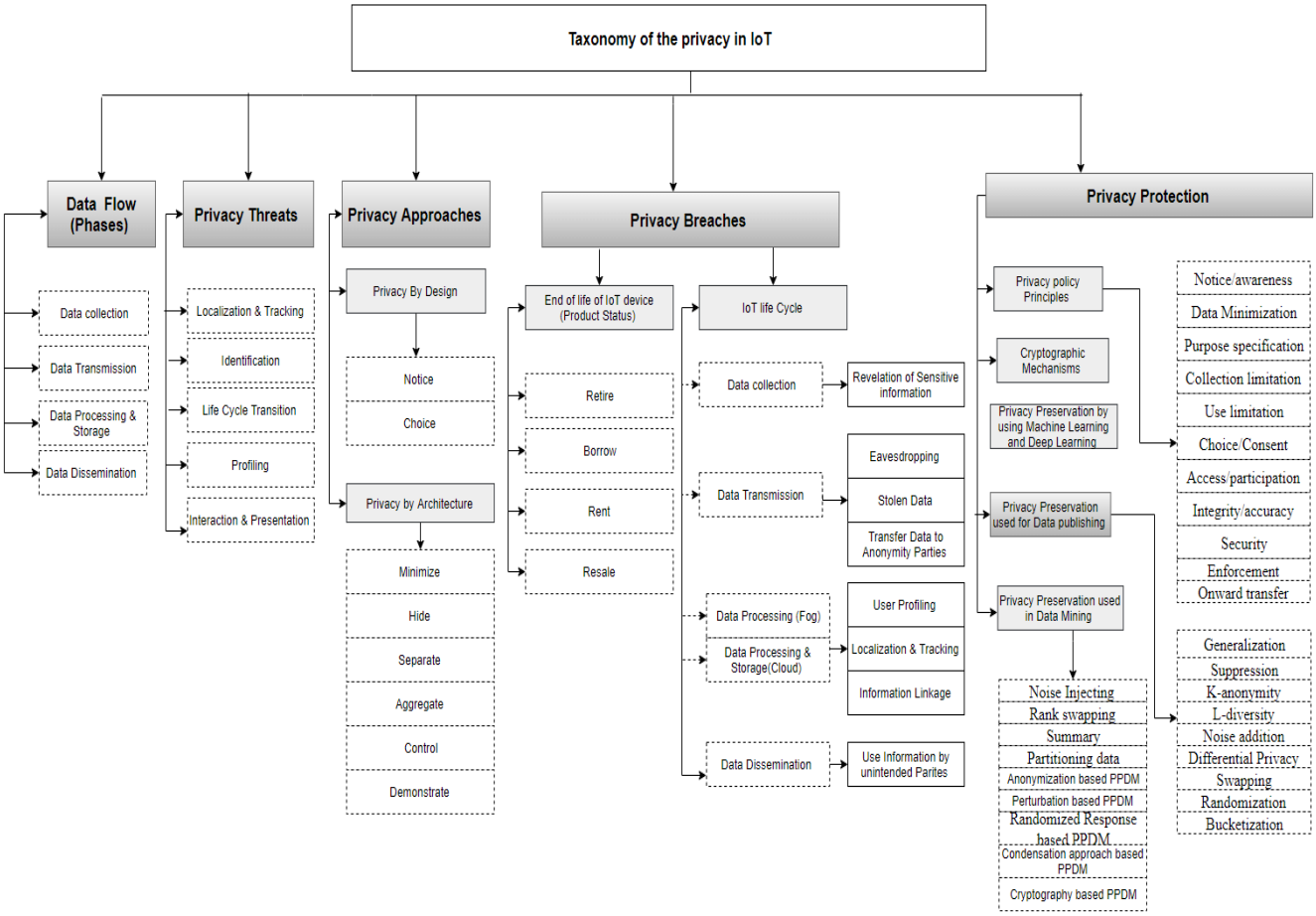

Figure 11. Taxonomy of IoT Data Privacy

9. CONCLUSION

The Internet of things (IoT) plays a vital role in many critical sectors nowadays, such as health-care, military, environment, etc. There is no doubt that IoT changes the way we live and work as all things surrounding us have become smart in performing tasks. The essence of IoT is sensing the environment around us and providing useful knowledge and services. However, the persuasive nature of data collection by IoT devices leads to privacy concerns that put its users at risk. Privacy concerns impact the acceptance of IoT technology by users. Thus, this study was conducted to carry out an in-depth investigation into the topic of privacy in IoT generally and IoT in healthcare in particular. It discussed privacy concerns of IoT in critical fields such as healthcare, military, and automobiles. It focused on discussing the privacy concerns in different IoT data flow (data collection stage, data transformation, data storage and processing, data dissemination). Moreover, the focus was on providing deep insight into data privacy across IoT-based healthcare. The outcomes of the investigation accomplished in the paper revealed that the privacy concerns in IoT can occur in different phases of IoT data flow. A complete scenario of IoT data flow was provided to convey a comprehensive understanding of the privacy concerns in IoT generally and IoT-based healthcare specifically. Furthermore, the paper summarized the privacy preservation mechanisms used in other fields that share the same nature of dealing with data collection and data processing. There is an inevitable need to design privacy preservation mechanisms for each phase in IoT-based healthcare to mitigate its concerns. Future research will extend this work to design a data privacy preservation technique that can suit IoT-based healthcare.

FUTURE WORK

Privacy is considered as the biggest obstacle in IoT. Many privacy issues are threatening individuals. Thus, privacy concerns impact the acceptance of IoT by healthcare beneficiaries. Therefore, there is a need to design a privacy preservation mechanism that can preserve a patient's privacy across IoT-based healthcare. In each IoT data phase, the privacy mechanisms should consider various issues such as the privacy approach, the data volume, data sensitivity, data mobility, data sources, and data types.

ACKNOWLEDGMENT

This work was supported by Omental as a part of the project [code: EG/SQU-OT /18/02] under the title of "Internet of Things (IoT) security and privacy aspects related to architecture, connectivity and collected data.

REFERENCES

[1] M. Xu, J. M. David, and S. H. Kim, "The Fourth Industrial Revolution: Opportunities and Challenges," *Int. J. Financ. Res.*, vol. 9, no. 2, p. 90, 2018.

[2] Z. Guangli, Z. Gang, L. Ming, Y. Shuqin, L. Yali, and Y. Xiongfei, "Prediction of the Fourth Industrial Revolution Based on Time Series," in *Proceedings of the 2018 International Conference on Intelligent Information Technology*, 2018, pp. 65–69.

[3] Z. K. Aldein Mohammeda and E. S. Ali Ahmed, "Internet of Things Applications, Challenges and Related Future Technologies," no. February, 2017.

[4] a Zanella, N. Bui, a Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, 2014, doi: 10.1109/JIOT.2014.2306328.

[5] A. Kott and I. Linkov, "Cyber Resilience of Systems and Networks," pp. 381–401, 2019, doi: 10.1007/978-3-319-77492-3.

[6] M. Hepp, K. Siorpaes, and D. Bachlechner, "Harvesting Wiki Consensus: Using Wikipedia Entries as Vocabulary for Knowledge Management," *IEEE Internet Comput.*, vol. 11, no. 5, pp. 54–65, Sep. 2007, doi: 10.1109/MIC.2007.110.

[7] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," *Inf. Syst. Front.*, vol. 17, no. 2, pp. 243–259, 2015, doi: 10.1007/s10796-014-9492-7.

[8] A. Mohsen Nia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," *IEEE Trans. Emerg. Top. Comput.*, vol. 5, no. 4, pp. 1–1, 2016, doi: 10.1109/TETC.2016.2606384.

[9] A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things—A survey of topics and trends," *Inf. Syst. Front.*, vol. 17, no. 2, pp. 261–274, 2015, doi: 10.1007/s10796-014-9489-2.

[10] M. Wu, T. J. Lu, F. Y. Ling, J. Sun, and H. Y. Du, "Research on the architecture of Internet of Things," *ICACTE 2010 - 2010 3rd Int. Conf. Adv. Comput. Theory Eng. Proc.*, vol. 5, pp. 484–487, 2010, doi: 10.1109/ICACTE.2010.5579493.

[11] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Cla, "Middleware for internet of things: A survey," *IEEE Internet Things J.*, vol. 3, no. 1, pp. 70–95, 2016, doi: 10.1109/JIOT.2015.2498900.

[12] Zhihong Yang, Yufeng Peng, Yingzhao Yue, Xiaobo Wang, Yu Yang, and Wenji Liu, "Study and application on the architecture and key technologies for IOT," *2011 Int. Conf. Multimed. Technol.*, pp. 747–751, 2011, doi: 10.1109/ICMT.2011.6002149.

[13] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, 2018, doi: 10.1016/j.jisa.2017.11.002.

[14] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "On the integration of cloud computing and internet of things," in *Future internet of things and cloud (FiCloud), 2014 international conference on*, 2014, pp. 23–30.

[15] D. N. Preethi, "Performance evaluation of IoT result for machine learning," *Trans. Eng. Sci.*, vol. 2, no. 11, 2014.

[16] S. S. Kulkarni, S. G. Kulkarni, and V. P. Datar, "Current Trends in Internet of Things: A Survey," 2018.

[17] I. F. Akyildiz and J. M. Jornet, "The internet of nano-things," *IEEE Wirel. Commun.*, vol. 17, no. 6, 2010.

[18] B. Katole, M. Sivapala, and V. Suresh, "Principle Elements and Framework of Internet of Things," *Int. J. Eng. Sci.*, vol. 3, no. 5, pp. 24–29, 2013.

[19] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Futur. Gener. Comput. Syst.*, 2018, doi: 10.1016/j.future.2018.04.027.

[20] A. Jacobsson, "IoT, Security and Privacy," *2018 1st Int. Conf. Comput. Appl. Inf. Secur.*, pp. 1–14, 2017.

[21] M. Abomhara, "Security and Privacy in the Internet of Things : Current Status and Open Issues," *Priv. Secur. Mob. Syst. (PRISMS), 2014 Int. Conf.*, pp. 1–8, 2014, doi: 10.1109/PRISMS.2014.6970594.

[22] D. Chen, P. Bovornkeeratiroj, D. Irwin, and P. Shenoy, "Private memoirs of IoT devices: Safeguarding user privacy in the IoT Era," *Proc. - Int. Conf. Distrib. Comput. Syst.*, vol. 2018–July, pp. 1327–1336, 2018, doi: 10.1109/ICDCS.2018.00133.

[23] J. Manyika *et al.*, "Unlocking the potential of the Internet of Things | McKinsey," 2015. [Online]. Available: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world. [Accessed: 06-Nov-2018].

[24] J. Kim and J. W. Lee, "OpenIoT: An open service framework for the Internet of Things," *2014 IEEE World Forum Internet Things, WF-IoT 2014*, pp. 89–93, 2014, doi: 10.1109/WF-IoT.2014.6803126.

[25] I. Ali, E. Khan, and S. Sabir, "Privacy-Preserving Data Aggregation in Resource-Constrained Sensor Nodes in Internet of Things: A Review," *Futur. Comput. Informatics J.*, 2017, doi: 10.1016/j.fcij.2017.11.004.

[26] A. Al-Fuqaha *et al.*, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," vol. 17, no. 4, 2015, doi: 10.1109/COMST.2015.2444095.

[27] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: The internet of things architecture, possible applications and key challenges," *Proc. - 10th Int. Conf. Front. Inf. Technol. FIT 2012*, pp. 257–260, 2012, doi: 10.1109/FIT.2012.53.

[28] I. Yaqoob *et al.*, "Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges," *IEEE Wirel. Commun.*, vol. 24, no. 3, pp. 10–16, 2017, doi: 10.1109/MWC.2017.1600421.

[29] R. Davies, "The Internet of Things opportunities and challenges," *Eur. Parliam. Res. Serv.*, 2015.

[30] F. Mattern and C. Floerkemeier, "From the Internet of Computers to the Internet of Things," in *From active data management to event-based systems and more*, Springer, 2010, pp. 242–259.

[31] E. T. Chen, "The Internet of Things: Opportunities, Issues, and Challenges," in *The Internet of Things in the Modern Business Environment*, IGI Global, 2017, pp. 167–187.

[32] B. L. R. Stojkoska and K. V Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," *J. Clean. Prod.*, vol. 140, pp. 1454–1464, 2017.

[33] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, "A survey on facilities for experimental internet of things research," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 58–67, 2011.

[34] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. Mccann, and K. Leung, "A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities," *IEEE Wirel. Commun.*, vol. 20, no. 6, pp. 91–98, 2013.

[35] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 3–9, 2014.

[36] H. Wang, Z. Zhang, and T. Taleb, "Editorial: Special Issue on Security and Privacy of IoT," 2017, doi: 10.1007/s11280-017-0490-9.

[37] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, 2017.

[38] E. Commission, "Internet of Things Factsheet Privacy & Security," *Eur. Comm.*, pp. 1–9, 2013.

[39] W. Ashford, "APIs key to security of internet of things, says Axway," *computerweekly.com*, 2013. [Online]. Available: https://www.computerweekly.com/news/2240209213/APIs-key-to-security-of-internet-of-things-says-Axway. [Accessed: 24-Sep-2018].

[40] M. Togan, B.-C. Chifor, I. Florea, and G. Gugulea, "A smart-phone based privacy-preserving security framework for IoT devices," in *2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2017, pp. 1–7, doi: 10.1109/ECAI.2017.8166453.

[41] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and Privacy in Smart City Applications: Challenges and Solutions," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 122–129, 2017, doi: 10.1109/MCOM.2017.1600267CM.

[42] S.-R. Oh and Y.-G. Kim, "Security Requirements Analysis for the IoT," *2017 Int. Conf. Platf. Technol. Serv.*, pp. 1–6, 2017, doi: 10.1109/PlatCon.2017.7883727.

[43] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 544–546, 2018, doi: 10.1016/j.future.2017.07.060.

[44] V. Adat and B. B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture," *Telecommun. Syst.*, vol. 67, no. 3, pp. 423–441, 2018, doi: 10.1007/s11235-017-0345-9.

[45] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wirel. Networks*, vol. 20, no. 8, pp. 2481–2501, 2014, doi: 10.1007/s11276-014-0761-7.

[46] C. Hall, "Secure IoT Through Oversight, Open Source and Open Standards," 2016. [Online]. Available: http://www.itprotoday.com/security/secure-iot-through-oversight-open-source-and-open-standards. [Accessed: 27-Jun-2018].

[47] N. Madaan, M. A. Ahad, and S. M. Sastry, "Data integration in IoT ecosystem: Information linkage as a privacy threat," *Comput. Law Secur. Rev.*, vol. 34, no. 1, pp. 125–133, 2018, doi: 10.1016/j.clsr.2017.06.007.

[48] C. P. Mayer, G. Editors, M. Wagner, D. Hogrefe, K. Geihs, and K. David, "Security and Privacy Challenges in the Internet of Things," *Electron. Commun. EASST*, vol. 17, 2009.

[49] R. C. Staudemeyer, H. C. Pohls, and M. Wojcik, "The Road to Privacy in IoT: Beyond Encryption and Signatures, Towards Unobservable Communication," *2018 IEEE 19th Int. Symp. "A World Wireless, Mob. Multimed. Networks,"* no. March, pp. 14–20, 2018, doi: 10.1109/WoWMoM.2018.8449779.

[50] C. Perera, C. Mccormick, A. K. Bandara, B. A. Price, and B. Nuseibeh, "Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms," 2016, doi: 10.1145/2991561.2991566.

[51] A. Rauf, R. A. Shaikh, and A. Shah, "Security and privacy for IoT and fog computing paradigm," *2018 15th Learn. Technol. Conf.*, pp. 96–101, 2018, doi: 10.1109/LT.2018.8368491.

[52] S. Sharma, K. Chen, and A. Sheth, "Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems," *IEEE Internet Comput.*, vol. 22, no. 2, pp. 42–51, 2018, doi: 10.1109/MIC.2018.112102519.

[53] A. A. Abi Sen, F. A. Eassa, K. Jambi, and M. Yamin, "Preserving privacy in internet of things: a survey," *Int. J. Inf. Technol.*, vol. 10, no. 2, pp. 189–200, 2018, doi: 10.1007/s41870-018-0113-4.

[54] W. Z. Khan, M. Y. Aalsalem, and M. K. Khan, "Five acts of consumer behavior: A potential security and privacy threat to Internet of Things," *2018 IEEE Int. Conf. Consum. Electron. ICCE 2018*, vol. 2018–Janua, pp. 1–3, 2018, doi: 10.1109/ICCE.2018.8326124.

[55] S. Chabridon *et al.*, "A survey on addressing privacy together with quality of context for context management in the Internet of Things," vol. 69, pp. 47–62, 2014, doi: 10.1007/s12243-013-0387-2.

[56] J. Bernal Bernabe, J. L. Hernández, M. V. Moreno, and A. F. Skarmeta Gomez, "Privacy-Preserving Security Framework for a Social-Aware Internet of Things," Springer, Cham, 2014, pp. 408–415.

[57] W. Li, T. Song, Y. Li, L. Ma, J. Yu, and X. Cheng, "A Hierarchical Game Framework for Data Privacy Preservation in Context-Aware IoT Applications," doi: 10.1109/PAC.2017.26.

[58] R. Boussada, M. E. Elhdhili, and L. A. Saidane, "Privacy Preserving Solution for Internet of things with Application to eHealth," doi: 10.1109/AICCSA.2017.75.

[59] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, "Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation," *Futur. Gener. Comput. Syst.*, vol. 76, pp. 540–549, 2017, doi: 10.1016/j.future.2017.03.001.

[60] K. Lueth, "Why it is called Internet of Things: Definition, history, disambiguation," *iot-analytics*, 2014. [Online]. Available: https://iot-analytics.com/internet-of-things-definition/. [Accessed: 12-Apr-2018].

[61] Lopez Research, "An Introduction to the Internet of Things (IoT)," *Lopez Res. Llc*, vol. Part 1. of, no. November, pp. 1–6, 2013.

[62] L. Tan, "Future internet: The Internet of Things," *2010 3rd Int. Conf. Adv. Comput. Theory Eng.*, pp. V5-376-V5-380, 2010, doi: 10.1109/ICACTE.2010.5579543.

[63] B. Insider, "IoT and IIoT are not a fad ; these technology," 2018.

[64] "IoT: number of connected devices worldwide 2012-2025 | Statista," *statista.com*, 2018. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. [Accessed: 25-Mar-2018].

[65] G. Chetty and M. Yamin, "Intelligent human activity recognition scheme for eHealth applications," *Malaysian J. Comput. Sci.*, vol. 28, no. 1, pp. 59–69, 2015.

[66] L. Sun, M. Yamin, C. Mushi, K. Liu, M. Alsaigh, and F. Chen, "Information analytics for healthcare service discovery," *J. Healthc. Eng.*, vol. 5, no. 4, pp. 457–478, 2014.

[67] M. Al-Ismail, T. Gedeon, and M. Yamin, "Effects of personality traits and preferences on M-learning," *Int. J. Inf. Technol.*, vol. 9, no. 1, pp. 77–86, 2017.

[68] A. Basahel and M. Yamin, "Measuring success of e-government of Saudi Arabia," *Int. J. Inf. Technol.*, vol. 9, no. 3, pp. 287–293, 2017.

[69] M. Yamin and O. O Al Harbi, "Online shopping adoption in Saudi Arabia: An empirical research," *Int. Multiling. Acad. J.*, vol. 2, no. 1, 2016.

[70] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the internet of things: Threats and challenges," *Secur. Commun. Networks*, vol. 7, no. 12, pp. 2728–2742, 2014, doi: 10.1002/sec.795.

[71] J. Pereira, "From autonomous to cooperative distributed monitoring and control: Towards the Internet of smart things," in *ERCIM Workshop on eMobility*, 2008.

[72] X. Li, Z. Xuan, and L. Wen, "Research on the architecture of trusted security system based on the internet of things," *Proc. - 4th Int. Conf. Intell. Comput. Technol. Autom. ICICTA 2011*, vol. 2, pp. 1172–1175, 2011, doi: 10.1109/ICICTA.2011.578.

[73] H. C. Hsieh and C. H. Lai, "Internet of things architecture based on integrated PLC and 3G communication networks," *Proc. Int. Conf. Parallel Distrib. Syst. - ICPADS*, pp. 853–856, 2011, doi: 10.1109/ICPADS.2011.73.

[74] J. Zhou *et al.*, "CloudThings: A common architecture for integrating the Internet of Things with Cloud Computing," *Proc. 2013 IEEE 17th Int. Conf. Comput. Support. Coop. Work Des. CSCWD 2013*, pp. 651–657, 2013, doi: 10.1109/CSCWD.2013.6581037.

[75] O. Salman, I. Elhajj, A. Kayssi, and A. Chehab, "An architecture for the Internet of Things with decentralized data and centralized control," *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. AICCSA*, vol. 2016–July, 2016, doi: 10.1109/AICCSA.2015.7507265.

[76] H. Guo, J. Ren, D. Zhang, Y. Zhang, and J. Hu, "A scalable and manageable IoT architecture based on transparent computing," *J. Parallel Distrib. Comput.*, 2017, doi: 10.1016/j.jpdc.2017.07.003.

[77] F. Alshohoumi, M. Sarrab, A. AlHamadani, and D. Al-Abri, "Systematic Review of Existing IoT Architectures Security and Privacy Issues and Concerns," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 7, pp. 232–251, 2019, doi: 10.14569/ijacsa.2019.0100733.

[78] F. Alshohoumi and M. Sarrab, "Critical Aspects Pertaining to Privacy Preservation of IoT Architecture.," in *Thirteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019)*, 2019, pp. 99–109.

[79] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad hoc networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[80] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. networks*, vol. 76, pp. 146–164, 2015.

[81] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl.*, vol. 84, pp. 25–37, 2017.

[82] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, "Vision and challenges for realising the Internet of Things," *Clust. Eur. Res. Proj. Internet Things, Eur. Commision*, vol. 3, no. 3, pp. 34–36, 2010.

[83] C. Li and B. Palanisamy, "Privacy in Internet of Things: from Principles to Technologies," *IEEE Internet Things J.*, vol. PP, no. c, pp. 1–1, 2018, doi: 10.1109/JIOT.2018.2864168.

[84] S. D. Warren and L. D. Brandeis, "The Harvard Law Review Association," *Harv. Law Rev.*, vol. 4, no. 5, pp. 193–220, 1890, doi: 10.1016/j.pmpp.2007.02.003.

[85] A. F. Westin, "Privacy and freedom," *Wash. Lee Law Rev.*, vol. 25, no. 1, p. 166, 1968.

[86] P. Kumaraguru and L. F. Cranor, *Privacy indexes: a survey of Westin's studies*. Carnegie Mellon University, School of Computer Science, Institute for Software Research International, 2005.

[87] N. Aleisa and K. Renaud, "Privacy of the Internet of Things: A Systematic Literature Review (Extended Discussion)," 2016.

[88] A. N. K. Zaman, "Privacy Preserving Data Sanitization and Publishing," 2017.

[89] I. Alqassem and D. Svetinovic, "A taxonomy of security and privacy requirements for the Internet of Things (IoT)," *IEEE Int. Conf. Ind. Eng. Eng. Manag.*, vol. 2015–Janua, pp. 1244–1248, 2014, doi: 10.1109/IEEM.2014.7058837.

[90] R. H. Weber, "Internet of Things - New security and privacy challenges," *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, 2010, doi: 10.1016/j.clsr.2009.11.008.

[91] J. S. Kumar, "A Survey on Internet of Things : Security and Privacy Issues," vol. 90, no. 11, pp. 20–26, 2014.

[92] D. He, R. Ye, S. Chan, M. Guizani, and Y. Xu, "Privacy in the Internet of Things for Smart Healthcare," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 38–44, 2018, doi: 10.1109/MCOM.2018.1700809.

[93] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of security and privacy issues of internet of things," *arXiv Prepr. arXiv1501.02211*, 2015.

[94] Z. Yan, P. Zhang, and A. V Vasilakos, "A survey on trust management for Internet of Things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, 2014.

[95] L. Stefanick, *Controlling knowledge: Freedom of information and privacy protection in a networked world*. Athabasca University Press, 2011.

[96] D. Chen, S. Barker, A. Subbaswamy, D. Irwin, and P. Shenoy, "Non-intrusive occupancy monitoring using smart meters," in *Proceedings of the 5th ACM Workshop on Embedded Systems For Energy-Efficient Buildings*, 2013, pp. 1–8.

[97] D. Chen, S. Kalra, D. Irwin, P. Shenoy, and J. Albrecht, "Preventing occupancy detection from smart meters," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2426–2434, 2015.

[98] S. Barker, S. Kalra, D. Irwin, and P. Shenoy, "Powerplay: creating virtual power meters through online load tracking," in *Proceedings of the 1st ACM Conference on Embedded Systems for Energy-Efficient Buildings*, 2014, pp. 60–69.

[99] D. Chen and D. Irwin, "Weatherman: Exposing weather-based privacy threats in big energy data," in *Big Data (Big Data), 2017 IEEE International Conference on*, 2017, pp. 1079–1086.

[100] D. Chen, S. Iyengar, D. Irwin, and P. Shenoy, "SunSpot: Exposing the Location of Anonymous Solar-powered Homes," in *Proceedings of the 3rd ACM International Conference on Systems for Energy-Efficient Built Environments*, 2016, pp. 85–94.

[101] R. Perez-Pena and M. Rosenberg, "Strava fitness app can reveal US military sites, analysts say," *New York Times*, vol. 29, 2018.

[102] N. Dragoni, A. Giaretta, and M. Mazzara, "The Internet of Hackable Things," in *Proceedings of 5th International Conference in Software Engineering for Defence Applications*, 2018, pp. 129–140.

[103] HP, "HP News - HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack," 2014. [Online]. Available: https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676. [Accessed: 18-Nov-2018].

[104] G. A. Fink, D. V Zarzhitsky, T. E. Carroll, and E. D. Farquhar, "Security and privacy grand challenges for the Internet of Things," in *Collaboration Technologies and Systems (CTS), 2015 International Conference on*, 2015, pp. 27–34.

[105] G. Sun, S. Huang, W. Bao, Y. Yang, and Z. Wang, "A privacy protection policy combined with privacy homomorphism in the internet of things," in *Computer Communication and Networks (ICCCN), 2014 23rd International Conference on*, 2014, pp. 1–6.

[106] P. Shayegh and S. Ghanavati, "Toward an approach to privacy notices in IoT," *Proc. - 2017 IEEE 25th Int. Requir. Eng. Conf. Work. REW 2017*, pp. 104–110, 2017, doi: 10.1109/REW.2017.77.

[107] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor, "A design space for effective privacy notices," in *Eleventh Symposium On Usable Privacy and Security (${$SOUPS$}$ 2015)*, 2015, pp. 1–17.

[108] S. Pape and K. Rannenberg, "Applying Privacy Patterns to the Internet of Things(IoT) Architecture," *Mob. Networks Appl.*, pp. 1–9, 2018.

[109] P. Bahirat, Y. He, A. Menon, and B. Knijnenburg, "A Data-Driven Approach to Developing IoT Privacy-Setting Interfaces," in *23rd International Conference on Intelligent User Interfaces*, 2018, pp. 165–176.

[110] N. Fotiou, V. A. Siris, A. Mertzianis, and G. C. Polyzos, "Smart IoT Data Collection," in *2018 IEEE 19th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, 2018, pp. 588–599.

[111] Tetsuya, I. Koichi, I. Hiroshi, T. Kenichi, A., and T. Ogura, "Privacy-protection Technologies for Secure Utilization of Sensor Data," 2014.

[112] S. Al-Fedaghi, "Engineering privacy revisited," *J. Comput. Sci.*, vol. 8, no. 1, pp. 107–120, 2012, doi: 10.3844/jcssp.2012.107.120.

[113] M. Gupta, *Handbook of research on social and organizational liabilities in information security*. IGI Global, 2008.

[114] N. Madaan, M. A. Ahad, and S. M. Sastry, "Data integration in IoT ecosystem: Information linkage as a privacy threat," *Comput. Law Secur. Rev.*, vol. 34, no. 1, pp. 125–133, 2018.

[115] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities," *IEEE Access*, vol. 5. pp. 26521–26544, 2017, doi: 10.1109/ACCESS.2017.2775180.

[116] E. Perrier, "Positive disruption: Healthcare, ageing and participation in the age of technology," *Sydney, NSW McKell Inst.*, 2015.

[117] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, "A medical healthcare system for privacy protection based on IoT," in *2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP)*, 2015, pp. 217–222.

[118] P. A. Laplante, M. Kassab, N. L. Laplante, and J. M. Voas, "Building caring healthcare systems in the internet of things," *IEEE Syst. J.*, vol. 12, no. 3, pp. 3030–3037, 2018.

[119] Amer, "Caregivers-and-Technology:what they want & need.," *2016*. [Online]. Available: https://www.coursehero.com/file/24894604/Caregivers-and-Technology-AARPpdf/. [Accessed: 28-Feb-2019].

[120] Z. Pang, "Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being," KTH Royal Institute of Technology, 2013.

[121] P. A. Laplante and N. L. Laplante, "A Structured approach for describing healthcare applications for the Internet of Things," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 2015, pp. 621–625.

[122] Alzheimer's association, "Alzheimer's Facts and figures Report | Alzheimer's Association," *2015*. [Online]. Available: https://www.alz.org/alzheimers-dementia/facts-figures. [Accessed: 28-Feb-2019].

[123] "Symptoms of Parkinson's disease," 2019. [Online]. Available: https://shakeitup.org.au/understanding- parkinsons/symptoms-of-parkinsons/. [Accessed: 13-Jan-2019].

[124] A. B. Pawar and S. Ghumbre, "A survey on IoT applications, security challenges and counter measures," *Int. Conf. Comput. Anal. Secur. Trends, CAST 2016*, pp. 294–299, 2017, doi: 10.1109/CAST.2016.7914983.

[125] S. M. R. Islam, D. Kwak, M. D. H. Kabir, M. Hossain, and K.-S. Kwak, "The internet of things for health care: a comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[126] M. Conti, N. Dragoni, and S. Gottardo, "Mithys: Mind the hand you shake-protecting mobile devices from ssl usage vulnerabilities," in *International Workshop on Security and Trust Management*, 2013, pp. 65–81.

[127] T. Ong, "Apple launches study to identify irregular heart rhythms on Apple Watch - The Verge," 2017. [Online]. Available: https://www.theverge.com/2017/11/30/16719458/apple-watch-study-irregular-heart-rhythms-stanford-university. [Accessed: 18-Nov-2018].

[128] K. Ozcan, … S. V.-I. T. H., and undefined 2017, "Autonomous Fall Detection With Wearable Cameras by Using Relative Entropy Distance Measure.," *ieeexplore.ieee.org*.

[129] P. Pierleoni, A. Belli, L. Palma, … M. P.-I. S., and undefined 2015, "A high reliability wearable device for elderly fall detection," *ieeexplore.ieee.org*.

[130] P. Laplante, N. Laplante, and J. Voas, "Considerations for healthcare applications in the internet of things," *Rel. Dig.*, vol. 61, no. 4, pp. 8–9, 2015.

[131] J. D. Bokefode, A. S. Bhise, P. A. Satarkar, and D. G. Modani, "Developing a secure cloud storage system for storing IoT data by applying role based encryption," *Procedia Comput. Sci.*, vol. 89, pp. 43–50, 2016.

[132] S. Janakiraman, S. Rajagopalan, and R. Amirtharajan, "Reliable Medical Image Communication in Healthcare IoT: Watermark for Authentication," in *Medical Data Security for Bioengineers*, IGI Global, 2019, pp. 1–26.

[133] S. Matwin, "Privacy-Preserving Data Mining Techniques: Survey and Challenges," Springer, Berlin, Heidelberg, 2013, pp. 209–221.

[134] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," *IEEE Internet Comput.*, vol. 21, no. 2, pp. 34–42, 2017, doi: 10.1109/MIC.2017.37.

[135] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," no. June, 2019.

[136] M. Restuccia, Francesco Tommaso, "Securing the Internet of Things in the Age of Machine Learning and Software-defined Networking 2018.pdf," vol. 1, no. 1, pp. 773–774, 2013.

[137] M. A. Al-garadi, A. Mohamed, A. Al-ali, X. Du, and M. Guizani, "Surveys," *Polit. Q.*, vol. 3, no. 4, pp. 581–589, 1932, doi: 10.1111/j.1467-923X.1932.tb01141.x.

[138] Y. Zhang, D. Zheng, and R. H. Deng, "Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2130–2145, 2018, doi: 10.1109/JIOT.2018.2825289.

[139] "InPen Smart Pen & Mobile App | Easy Diabetes Management Companion Medical," 2019. [Online]. Available: https://www.companionmedical.com/InPen. [Accessed: 08-May-2019].

[140] "Home - VitalConnect," 2019. [Online]. Available: https://vitalconnect.com/. [Accessed: 08-May-2019].

[141] "Sleep Tracking Mat - Sleep | Withings," 2019. [Online]. Available: https://www.withings.com/us/en/sleep. [Accessed: 08-May-2019].

[142] "Dexcom G5 Mobile CGM System | continuous glucose monitoring on your smart device," 2019. [Online]. Available: https://www.dexcom.com/g5-mobile-cgm. [Accessed: 12-May-2019].

[143] "Privacy Policy | Animas® Insulin Pumps & CGMs | Animas® US," 2019. .

[144] "AliveCor," 2019. [Online]. Available: https://www.alivecor.com/. [Accessed: 12-May-2019].

[145] "MyNotifi," 2019. [Online]. Available: https://www.mynotifi.com/. [Accessed: 08-Jul-2019].

[146] "Privacy Policy - Qardio," 2019. [Online]. Available: https://www.getqardio.com/privacy-policy/. [Accessed: 14-Jul-2019].

[147] "Zio Patch Cardiac Monitoring: iRhythm Technologies," 2019. [Online]. Available: https://www.irhythmtech.com/professionals/why-zio. [Accessed: 09-Jul-2019].

[148] A. Chacko and T. Hayajneh, "Security and Privacy Issues with IoT in Healthcare," *EAI Endorsed Trans. Pervasive Heal. Technol.*, vol. 0, no. 0, p. 155079, 2018, doi: 10.4108/eai.13-7-2018.155079.

[149] K. Mivule and C. Turner, "Applying Data Privacy Techniques on Tabular Data in Uganda."

[150] B.-C. Chen, D. Kifer, K. LeFevre, and A. Machanavajjhala, *Privacy-Preserving Data Publishing*, vol. 2, no. 1–2. 2009.

[151] A. Majeed, "Attribute-centric anonymization scheme for improving user privacy and utility of publishing e-health data," *J. King Saud Univ. - Comput. Inf. Sci.*, 2018, doi: 10.1016/j.jksuci.2018.03.014.

[152] M. B. Malik, M. A. Ghazi, and R. Ali, "Privacy Preserving Data Mining Techniques: Current Scenario and Future Prospects," *2012 Third Int. Conf. Comput. Commun. Technol.*, pp. 26–32, 2012, doi: 10.1109/ICCCT.2012.15.

Mohamed Sarrab is currently working as a researcher and Deputy Director of Communication and Information Research Center, Sultan Qaboos University. He obtained his Ph.D. degree in Computer Science from De Montfort University, UK. His research interests are in areas of software engineering, information privacy, computer security, Runtime Verification, and Information Flow Control. He is also interested in computer forensics, mobile applications, open-source software. He is a senior member of the IEEE.

Fatma Nasser Alshohoumi. Ph.D. student in the Computer Science Department, College of Science. She is also Research Assistant at Communication and Information Research Center, Sultan Qaboos University (SQU). She obtained her MS.c. in Computer Science from Sultan Qaboos University. Her research is in areas of Software engineering, Information Privacy, IoT security and Information Flow control in Healthcare applications

APPENDIX

Table IV: Some of the privacy preservation mechanisms used for data publishing

Privacy techniques for data publishing	Description
Generalization	Attributes that could cause identity disclosure are made less informative; sensitive values are replaced with a general none revealing value. An example includes replacing the gender attribute value with "person" instead of "Male" or "Female". [149][150][151].
Suppression	It is a popular data privacy method in which data values that are unique and can be used to establish an individual's identity are omitted from the published data set[149]. Replacing some attribute values (or parts of attribute values) by a special symbol that indicates that the value has been suppressed (e.g., "*" or "Any").[150][151]
K-anonymity	Utilizes generalization, and suppression. K-anonymity requires that for a data set with quasi-identifier attributes in the database to be published, values in the quasi-identifier attributes be repeated at least k times to ensure privacy. [149]
L-diversity	Is an extension of k-anonymity that seeks to prevent information leak attacks on homogenous attributes [149]
Noise addition	Is a data privacy procedure defined by Kim [1986], in which a random numeric value (noise) is added to confidential numeric data values to provide information concealment?[149]
Differential Privacy	The perturbation technique that has recently gained attention in data privacy research, is a process in which Laplace noise is added to a query response such that the presence or absence of an individual cannot be observed.[149]
Swapping	The swapping mechanism produces a release candidate by swapping some attribute values.[150]
Bucketization	Produces a release candidate by first partitioning the original data table into non-overlapping groups (or buckets) and then, for each group, releasing its projection on the non-sensitive attributes and also its projection on the sensitive attribute.[150]
Randomization	A release candidate of the randomization mechanism is generated by adding random noise to the data. [150][151]

Table V. Some of privacy preservation mechanism for data mining

Privacy-Preserving Data Mining Techniques	**Description**
Noise injecting	Perturbative methods: A different set of methods protecting against disclosure of the value of sensitive attribute [133].An attribute is systematically changed by adding to a value (noise-injecting)obtained from a probability distribution
Rank swapping	The main idea is to swap the values of a given attribute among records in a dataset.[133]
Summary	An ultimate method for protection against attribute disclosure is based on the idea that the original data is replaced, in its entirety, by a synthetic dataset with the same statistical properties (e.g. Mean, variance, etc.) As the ones of the original dataset. [133]
Partitioning data	The partitioning may be either vertical or horizontal. [133]
Anonymization based PPDM	This refers to an approach where the identity or/and sensitive data about record owners are to be hidden. Replacing a value with less specific but semantically consistent value is called as generalization and suppression involves blocking the values.[152]
Perturbation based PPDM	The original values are replaced with some synthetic data values so that the statistical information computed from the perturbed data does not differ from the statistical information computed from the original data to a larger extent.[152]
Randomized Response based PPDM	The information received from each individual user is scrambled and if the number of users is significantly large, the aggregate information of these users can be estimated with a good amount of accuracy. [152]
Condensation approach based PPDM	Constructs constrained clusters in the dataset and then generates pseudo-data from the statistics of these clusters.[152]
Cryptography based PPDM	Cryptographic techniques are ideally meant for such scenarios where multiple parties collaborate to compute results or share nonsensitive mining results and thereby avoiding disclosure of sensitive information. [152]