International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V70I2P207

Volume 70 Issue 2, 43-52, February, 2022

Original Article

A study of Data Privacy in Internet of Things using Privacy Preserving Techniques with its Management

N. Krishnaraj[1], S. Sangeetha[2]

[1]*Associate Professor, Department of Networking and Communications, School of Computing, SRM Institute of Science and Technology, Kattankulathur, Tamilnadu, India.*

[2]*Assistant Professor, Department of Computer Science and Engineering, Veltech Multitech Dr Rangarajan Dr Sakunthala Engineering College, Chennai, Tamilnadu, India*

[1]*drnkrishnaraj@gmail.com,* [2]*sangee2723@gmail.com*

Abstract *- The living standards of human lives in societies are enhanced and move towards sophisticated automation by implementing the Internet of Things (IoT) in their daily life. However, limited storage, power and computational capabilities are presented in IoT devices. Hence, users' data are collected using various devices, and they can be modified and sent to the clouds. People can access the data from anywhere and anytime due to access credentials, and this leads to problems such as an explosion of sensitive information and loss of trust between parties. Privacy and security issues are raised from this explosion of users' personal information over the IoT environment, and this must be addressed. However, researchers focused on this as a major concern for IoT. In this research work, the explanation of data privacy is given, and in order to fulfil its requirements, privacy-preserving techniques are studied. Differential privacy is the most widely used technique to ensure the user's data privacy, which is also discussed in this work. Before uploading any data to cloud storage, it must be encrypted using cryptographic techniques, where the importance of these techniques are also presented in the survey. More data are collected via wearable devices in IoT, and its challenges along with privacy management are given in the study. Finally, the threats and major challenges of privacy with its future directions about IoT based applications' privacy is explained.*

Keywords - *Internet of Things, Data Privacy, Security, Privacy Preserving Techniques, Differential Privacy, Challenges.*

I. INTRODUCTION

An IoT-based smart application is designed over many traditional applications because of the IoT technology development. According to the architecture, much work has been developed using applications based on IoT. However, the issues of security and privacy are not resolved. While creating the IoT applications, namely protection of data and authentication [1], the most difficult part is the privacy and security, where machine learning (ML), fog computing and blockchain are designed to resolve these stated issues.

A secure framework of a smart healthcare system is designed by Jaiswal et al. [2] by using the data collection process. The critical patients are monitored by using an intelligent device in a smart healthcare system. Using either wire or wireless systems are connected with this sensor device, where this can be accessed remotely in some applications. Bluetooth, Wifi or Zigbee can be used here for connectivity purposes, but various attacks are injected into every device for modifying sensitive information. Existing algorithms or protocols are not appropriate for solving security issues due to resource constraint devices. Therefore, lightweight protocols are required for IoT devices, where Satapathy et al. [3] designed an elliptic curve cryptography (ECC) algorithm and used the small key size for IoT applications.

Three layers such as network, application and physical layers are used to develop the IoT architecture, where a vast amount of IoT smart devices are deployed in physical layers for the application process. From the environment, numerous data is collected from IoT devices. Using the following three steps, the data collection process is carried out:

1) The first step is the collection process of information, where raw data are collected from smart sensor devices and then transferred for further process.
2) To get the information, the collected data are aggregated for the next processing.
3) From this aggregated data, some techniques apply various analyses to extract meaningful information as per applications of IoT.

Although a collection of data and processing is an important part of the implementation of IoT, privacy issues arise during these data collection stages. For instance, if an attacker receives information about a patient's profile, the IoT activates a hospital setting to create a pool of patients. Privacy protection technologies must be designed to address the privacy issue of the IoT system.

II. DIFFERENTIAL PRIVACY AS DP

Researchers accepted DP as one of the strict models in terms of privacy protection, where the existing algorithm called k-anonymity [4] is still problematic, and therefore

DP is designed. Various privacy uses very strict restrictions and definitions. An interference noise is added in the published data to protect the privacy information of a potential user. An attacker cannot obtain this information, even though he knows some information. Hence, DP eliminates the disclosure of this privacy information, which is shown in Fig. 1.

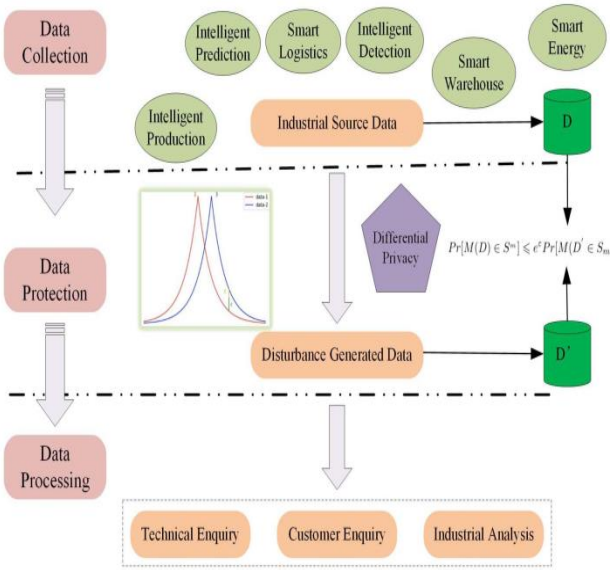

Fig. 1 IoT model with DP

Without revealing sample details, an analysis of the entire data is completed by using DP, which is the major goal of this technique. On the other hand, it can counter the background knowledge of different privacy attackers. According to a solid mathematical foundation, DP measures the privacy protection memory.

A. DP's basic definitions

Consider M as a random algorithm, pair of an adjacent dataset as D and D' and set of all values as P_m and a subset of P_m as S_m for that algorithm. Finally, the algorithm M should satisfy as follows:

$$\Pr[M(D) \in S_m] \leq e^{\varepsilon} \Pr[M(D') \in S_m] \quad (1)$$

Then, DP is satisfied by the algorithm M and budget of privacy protection is ε.

B. DP's progress with the development

The extension of DP is developed for solving the issues of privacy. These developments are designed based on the changes in the application of information technology. For instance, new requirements are needed for sensor data privacy protection due to the popularity of IoT and therefore, it reaches a constant development in this direction. The development of DP can be summarized, and various researchers studied the progress, and it is reviewed in this work as below:

Xiao et al. [5] Different specificities were tried based on bandwidth changes, and better results were obtained. Fudd et al. [6] Another privacy system based on supermodules has been proposed, which is valid in data anonymization. For personal differential specificity, Soria-Comas et al. proposed to establish the use and protection of various privacy safeguards in [7].

Wang et al. [8] Developed by CTS-DP, the relevant time range can be used for data output on another privacy basis. Goryczka Xiong [9] made extensive comparisons of various security add-ons while implementing DP. At the same time, Zhang et al. [10], a study based on the dynamic specificity of ADMM-based distributed classification, has been resolved. In addition, Kao et al. [11] Various privacy measures for continuous data output using temporary contacts.

C. Implementation Mechanisms

In order to provide a DP's protection, the implementation of DP and noise adding process is the major technology. From the point of view of engineering technology, there are 2 categories for the implementation of DP such as exponential and Laplace mechanisms. For numerical results, the mechanism of Laplace is more suitable, and for non-numerical results, an exponential mechanism is highly acceptable [12].

1) Mechanisms of Laplace Mechanism: Consider the function as $f : D \rightarrow R^d$, dataset as D function sensitivity as Δfthen protection of DF is provided by a random algorithm as $M(D) = f(D) + Y$. Random noise is added and considered as $Y \rightarrow Lap(\Delta f/\varepsilon)$ that obeys this distribution with the parameter called $\Delta f/\varepsilon$..

$$M(D) = f(D) + \left(Lap_1\left(\frac{\Delta f}{\varepsilon}\right), Lap_2\left(\frac{\Delta f}{\varepsilon}\right), \ldots, Lap_d\left(\frac{\Delta f}{\varepsilon}\right) \right)^T \quad (2)$$

The optimal upper bound with queries is discussed by Li et al. [13] for the mechanism of Laplace under DP.

2) Mechanism of Exponential: M is the input algorithm with D dataset and achieved the output or availability function as $r \in Range, q(D, r)$, where Δq is considered as the sensitivity for the function $q(D, r)$. All possible values can be normalized only when the M is proportional to e $\mathrm{xp}([\varepsilon q(D, r)]/[2\Delta q])$ probability for getting the corresponding value, and finally, the protection of DP is achieved.

III. PRIVACY-PRESERVING TECHNIQUES IN IOT

A piece of sensitive information such as personal data, medical data, actual user location and so on are collected and analysed by various IoT services. Lack of privacy protection activities and methods can lead to serious privacy leaks.

Different types of privacy-preserving techniques are described in the following sections:

- ❖ Basic and naive approaches are represented in general approaches for k-anonymity [14] and data privacy, which will be useful for enhancing the protection using encryption, masking the data and pseudonyms.
- ❖ A technique that needs an encryption scheme without the need for decryption models using ciphertexts to provide security is known as homomorphic encryption.

Here, the data of end-users remain secret to the service providers and third parties, which is highly enhanced privacy protection.

- ❖ Signer anonymity and security are highly provided by using the advanced digital signature schemes that are represented in two signatures, such as ring (RS) and group signatures (GS).
- ❖ Without revealing a user's identity, an attribute possession, i.e. age, membership of users, etc., is proved by enabling the digital signature schemes called Attribute-based Signatures (ABS). According to the user's attributes, encryption and decryption of user data are enabled by Attribute-based encryption (ABE).

A. General approaches

Sensitive data is encrypted to enable the basic privacy status. The compromised data encryption prevents passive attackers from accessing the content, which leads to the connection. A common secret key is shared, and two communication nodes trust each other for symmetric data encryption such as IDEA, AES, XTEA, which can be applied in this approach. Securely this secret key is pre-distributed or established. The techniques such as RSA ElGamal are used as asymmetric encryption schemes that are used to encrypt the data with the help of public keys. However, the estimated cost of these programs prevents them from spreading to IoT systems using controlled devices. SMS messages and secret keys are encrypted by using the common scheme called asymmetric encryption schemes. A single plaintext is encrypted to multiple ciphertexts using the ElGamal scheme that provides unsinkability, and this is considered as the most needed solution for privacy-preserving. An identity disclosure is protected by the k-anonymity approach, but the same approach is not sufficient for attribute disclosure as given in [15].

The location sharing mechanism is proposed for privacy preservation by Shen et al. [16], where sensitive private information is hidden by employing the blooming filter [17]. In IoT, privacy is preserved by developing a context-aware policy work that is discussed in [18]. According to semantic rules, the framework makes the policies includes the location of closeness, hiding, granularity, cloaking, authorization and operational. The location data and user's privacy data is managed by employing the third-party auditor, but it is unable to disguise the users' identities because this algorithm does not have hashing and anonymity policies. The authors from [19] recently proposed an anonymous authentication program designed to engineer IoT systems. Their software sensor ensures features such as anonymity, detection, defence against replay attacks, cloning attacks, and mutual recognition. The program is simple because it uses hash functions. However, this plan does not address the reliability and privacy of data or any other security or privacy features (denial, withdrawal, etc.).

B. Encryption model based on Homomorphic

Encryption of sensitive data is carried out by homomorphic encryption, and here decryption process is not required by this process. Another party will process this encrypted data without the knowledge of what data is present in the files. There are two main types of symmetric ciphers: partial cipher (PHE) and full symmetric cipher (FHE). Several partially isomorphic ciphers exist, such as Paillier [20] or Benaloh [21]. However, some work, such as [22-24], shows that FHE encoders require large amounts of computing and memory. According to the study [25], symmetric ciphers may be part of a multidisciplinary secure computation, creating new opportunities for ubiquitous applications to protect development privacy.

C. Signatures based on Ring and Group

Typical digital signature programs are usually interconnected and can be identified by a user ID. When user identity is separated from the verification process, user privacy, authentication, and affiliation are guaranteed. Instead of groups, the user themselves provides authentication by signing a message without user identities or certificates and transforming it to a verifier anonymously is called GS. A group secret number key is used for producing the signature, and one public group key is used for verification, which is spread over the system.

D. ABE and ABS

Signatures are generated without leaking more information for satisfying a policy using ABS schemes. Services or data are requested by the user for generating the signatures with the help of attributes. Among all users, signers are indistinguishable and anonymous. Signers cannot forge signatures with attributes they do not possess. Messages sent within the IoT infrastructure can only be recognized by a user with valid attributes.

An attribute tree is employed and uses the policies of OR, AND and threshold gates by implementing the ABS scheme in [26]. According to the tree size, the operations such as 2l bilinear pairing and few exponentiations are used for signature verification, where 2l+2 is the signature length. But, this model is applied to only IoT privacy services due to bilinear and exponentiation.

A protocol of decentralized anonymous authentication is proposed by Alcaide et al. [27] and sends the data to the collector of IoT. Secret sharing, threshold cryptography and proof of zero-knowledge techniques are used to combine the anonymous credentials. Various exponentiation operations are contained in this protocol, which is compatible with the most powerful operating systems. However, this protocol is insecure, which is proved by Lin et al. [28]. The competitor can deceive data collectors by pretending to be a legitimate user.

IV. CRYPTOGRAPHY

The performance of cryptographic primitives operations in terms of arithmetic operations are discussed in this section that is used in the implementation of IoT for security solutions.

We process and measure functionality on a variety of platforms, including microcontrollers, smart cards, and smartphones used in the environment of IoT. Some of the techniques such as Secure Hash algorithms as SHA-1 and SHA-2, RSA, Advanced Encryption Standard as AES,

generator functions for random numbers and cryptography such as the ECC and ECDSA programs. In various IoT security processes, these encryption alternatives and functions are used. In different protocols such as DTLS, OSCAR and Lithe-DTLS [29-31], data encryption is occurred by using AES.

The following techniques explain the tested schemes and cryptographic primitives:

In the ECB mode, symmetric cipher AES uses the 128-bit of plaintext for encryption using a 128-bit key, where 4256-bit and 8448-bit plaintexts are used by SHA-1 and SHA-2. A verification of RSA signature or data encryption process is carried out by RSA ver/enc 1024b and 2048b, where decryption process is taken care of by RSA sig/Dec 1024b and 2048b with 1024-bit and 2048-bit modulo. A function for random number generator is developed by using 160bit and 560bit random numbers. A bit of 128 Fp elliptic curves are used for the multiplication operation of the ECC algorithm

Table.1 shows the technical specifications of devices such as Recourse-constrained and high-performed cryptographic primitives. Expect single-board computer Raspberry Pi model and smartphone Nexus 5LG, MSP430F149, MSP430F6638, NXP JCOP CJ3A080v24 and ML3-36k-R1 uses the processor of 16-bit CPU with 8MHZ, 20MHz, 30MHz and 33MHz, where first two models, i.e. Raspberry Pi and smartphone uses the processor of 32-bit ARM of version 11 and 7 with single and Quad-core of 700MHz and 2260MHz.

V. WEARABLE DEVICES OF IOT FOR DATA COLLECTION

Wearable technology offers many benefits in the health environment, but the emergence of approved medical devices in health systems has been slow. A ball with data gloves and sensors is used to monitor finger movements in hand recovery therapy for stroke patients [32]. Sensitive wearable EMG sensors communication technology are used to measure and monitor electrical activity related to nerve and muscle conduction for affected tissues. In order to avoid MRI needs, sensors of optical are used for taking the neurons imaging of the brain. Additionally, the connective skin shape of these sensors improves the portability of sophisticated devices and enhances the bioelectrical signals received by users [34].

In patients with chronic obstructive pulmonary disease (COPD), autonomy may improve quality of life and reduce pulmonary hospitalization. Lightweight wireless pulse oximeters are commonly used in conjunction with COPD to detect blood-oxygen levels by analyzing live patient data [35–36]. Apple is FCA certified for its ECG and certified in the European Economic Area, and now the health feature can be used in more than 20 countries. In the UK, remote monitoring of people with symptoms of chronic illnesses is detected by using wearables that can provide doctors with the ability to remotely screen display important symptom data without fail [37].

Wearable gadgets, such as smartwatches, headphones, gloves, and other stiff structures, are attached to the wearer's body or clothing. Transmission mediums like Zigbee or Wi-Fi can be used to communicate with doctors in case of an accident or emergency. Using the wearer's physiological and functional data, the device captures and filters data from the user over a lengthy period of time. As the last step, the information collected by the sensor is sent to a powerful distant computer or cloud processor for processing. Communication networks make it possible to link sensors and control systems. In order to meet needs like always-on transmission services and short end-to-end latency, the 5G communication technology has been developed to improve broadband networks. Digital healthcare uses enhanced data to improve healthcare facilities and human health. Some examples of wearable data gathering devices may be seen in Fig. 2.

Table I. Devices' Technical Specifications.

Specifications	**Device Names**					
	MSP430F149	**MSP430F6638**	**NXP JCOP CJ3A080v24**	**ML3-36k-R1**	**Raspberry Pi model**	**Nexus 5 LG**
Size of RAM	60kB	18kB	6kB	1088+960B	512MB	2GB
Size of Storage	60kB	256kB	200+80kB	280+60kB	8GB	16GB
Designation	Microcontroller of 8MHz	Microcontroller of 20MHz	Java card of 30MHz	Multos card of 33MHz	ARM of 700MHz	ARM of 2260MHz

Fig. 2 Various Sensors used for data collection in IoT-smart healthcare [41-44].

A. Challenges in IoT

The safety and privacy of acquired data must be taken into account while using wearable technology. Various wearable gadgets store data on local storage without encrypting it or protecting it in any way. Thus, sensitive and personal health information is more likely to be lost. Bluetooth, NFC, or Wi-Fi are the most common methods of connecting wearable gadgets to a smartphone. Data cannot be protected against a vicious assault using just unprotected wireless communication channels [45]. Data from wearable sensors are always sent via cell phones, and third-party apps put on smartphones can be hacked. In wearable devices protection, two different types of privacy threats are involved, such as active and passive attacks, where personal information and password of users are obtained from smart devices is, known as passive attacks, and this attack will not disrupt the device of the target. But, the device is destroyed and changed by the active attacks. Due to security lack, user data is easily obtained by a possible intruder without the data owner's knowledge in a passive attack. Cameras and microphones built into wearable devices can raise data security threats. Microphones may violate privacy by filming unauthorized audio or recording others' audio without their permission [48-49]. An explosion of personal information of a user and current surroundings are carried out by hacking the wearable camera, but still, various people use these systems and violate the other's privacy.

An informed user is one who understands the data that their device is collecting and how it can be used to improve data security and privacy for others. Wearable devices may be protected by encrypting their data, enhancing security, and employing secure network interfaces to move data from wearable devices to a central storage location, among other methods. Local storage is able to provide many local storages [50]. Wearable gadgets can't be used without compromising data security. The danger of data loss can be mitigated, however, if these technologies are used properly.

B. Laws in IoT

IoT customers need to ensure that data is collected, stored and used in a way that is beneficial to them and does not harm their privacy. It is essential to reduce risk and build trust regardless of one's privacy concerns. Although they do not apply specifically to the IoT, many guidelines and regulations, particularly those applicable to European citizens, such as the Principles of Fair Practices (FIPPs) [51] and the General Data Protection Regulation (GDPR) [53]) already exist.

In order to comply with these rules and standards, organisations must be aware of the privacy hazards associated with the Internet of Things (IoT) technology. To summarise, the most significant sources of corporate privacy concerns are the data collected or generated, the data activities carried out on that data, and the context in which such personal data is gathered, created, processed, disclosed, and retained [52]. Thus, the GDPR specifies that personal data must be processed in accordance with the terms "requirements" and "data reduction." Transparency, advertising, and "consent" are all used in data operations and environmental regulation to gain customer consent [54]. Consumers can use privacy solutions to determine who is legally required to access and disclose their personal information. Some main risk factors play a part in general IoT difficulties, such as the size, dynamic changes, variety of devices, and IoT devices managed by resources.

a) Laws on personal data

A "natural person" is defined under the GDPR as any "individual" who may be identified or identified by reference to an identifier or to one or more characteristics distinctive to that individual, whether or whether that identifier or source is directly or indirectly linked to the data in question." [53].

There are two types of personal data:

(a) Voluntary statements are those made by the individual themselves.

(b) Transactional data collected from an individual's interaction with a business.

The output of data analysis, aggregation, or mining is speculative data, also known as derived data.

For customers to have access to their personal data, IoT systems must be open and transparent. Consumers have the right to examine and accept or withdraw their consent to the collection and use of their personal data [51]. "Internal or external" recognition isn't enough; consumers should have the ability to choose the data they want to share with the IoT system. Therefore, IoT devices must deal with data loss.

Personal data's integrity, availability and confidentiality must be ensured by solutions of security. For example, encryption is required when and when data is transmitted, which can be a challenge to support resource-controlled IoT devices [54]

b) Laws on Data Actions

The GDPR [56] requires that EU consumer consumers agree to a personal data processing agreement "through a clear and documented law that creates free, specific, informative and explicit information." All processing of this personal data must be consented to, and "silence, pre-selected boxes or inactivity" cannot be approved. Withdrawing should be as easy as giving consent.

Therefore, handling of personal data is required by consent of IoT systems since it includes a variety of systems, applications, networks and devices with different capabilities and different technologies. Each component of the IoT system must be approved to control the operation of the IoT. Higher risks are presented in the devices of IoT because they are highly connected with the cloud and within the Iot system and defined as resource-constrained. To address the need of various sub-systems of an IoT model, more than one authorization solution is deployed in the IoT system models. [54].

VI. MANAGEMENT IN PRIVACY

Privacy is complex and personal; Individuals have different opinions; however, it is important to support the responsibilities that democracy requires. Community laws are an important means of ensuring the protection of an individual's ability to freely exercise his or her rights.

Unfortunately, technological advancements, innovations, and sustainable changes that technology brings into our lives have reached a point where we cannot comply with the law [57]. In order to predict and develop the recent trends and marketing strategies, companies collect millions of facts about consumers with the help of IoT and big data. According to companies' strategies, they informed that these technologies are simply used to provide better services to the consumers. But, the main goal is to influence the decisions of costumers on the cost by analyzing their personal information because companies are interested in this decision influences of end-users.

A. Disclosure of Privacy

The importance of business transactions is evident in the IoT environment. As more devices are connected to a user, so does the convenience and usefulness of this tool [58], allowing users to search for anything from data, which is created from different devices of IoT and connected databases, offer undeniable advantages and risks to consumer privacy [59]. The most popular theory for exploring these transactions is privacy account theory, in which individuals disclose their personal information or interact with technology until the perceived benefits outweigh the risks and consequences [60]. The theory posits that individuals will perform a perceptual cost analysis based on the benefits of exposure and the negative effects that an individual may experience as a result of technology use [61]. The PCT has recently been used in the IoT environment. In their study of 508 Taiwanese citizens, [58] concerns about information privacy negatively affected intentions for continued IoT use, while perceived gains had a positive effect on intentions. In a study of American consumers, the report in [62] realizes the confidence, benefits, and risks of various applications of IoT such as smart transportation, smart home and healthcare system. With regard to health, privacy risks have a significant negative impact on the willingness to disclose personal data, while trust and perceived gains can positively influence choice. In the case of smart transportation and smart housing, the perceived and realized gains had a significant positive effect, but the risks identified were very low. Perceived earnings are the largest predictor of willingness to provide information on health and smart transportation, while trust is the largest predictor of smart homes. Empirical support for the use of PCT is provided by this study in an IoT environment and explain how positive emotions (i.e., trust and benefits) can negatively affect adoption, information disclosure, and negative emotions (i.e., risk and privacy).

Privacy policies are an important way for companies to express how consumer data is collected and used. It is said that privacy policies can reduce risk, increase control and increase trust. However, the privacy policies are long and hard to read, which makes the customer fail to understand the content. As a result, these disclosures go against the intended effect and raise concerns about control and risk. Hence, need for development for informing consumers in a better way, and the process of information used [65]. To combat these problems, researchers have developed privacy labels based on label approaches, and privacy labels can improve understanding of privacy practices [66] and create a sense of trust. This approach was recently revised to create privacy labels based on GDPR [68].

B. Privacy Metrics

We argue that in order to create an IoT-based privacy label, this latest research on privacy and the trust label must be used by IoT providers. It must create an understanding for the consumer of how information about the company is used and collected in accordance with privacy regulations, as well as create a positive sense of privacy as well as credibility. For example, in Europe, according to the GDPR, labels must contain the following information [69]:

1. Specify the data controller and contact details.
2. For the processing, legal basis and personal data are used.
3. Types of recipient end-user data.

4. Current details of security when conveying data to a third country.
5. Period of data retention.
6. Claims regarding data content: access to their data, editing, processing control, data deletion, data portability.
7. The right to withdraw consent at any time if data processing is subject to consent.
8. The right to file a complaint with the supervisory officer.
9. Identifying that personal data's disclosure is whether contractual or statutory requirements or the non-disclosure's consequences.
10. The logic, profiling and impact of such processing are the uses of the automated decision-making process.
11. Must need the data protection officer's contact details.
12. Further information processing

VII. THREATS AND CHALLENGES OF PRIVACY

With the development of the IoT and the spread of technology, the major problem is the confidentiality of user data. In an IoT environment, the common thing is the collection, usage and exchange of data. Here, the most common threats to IoT privacy [70] is discussed as follows:

A. The name and addresses of individuals can be identified by using the threats called identification. In the IT stage, references model' back-end services have this experience of this threat, where numerous information is stored in a server that is out of the object's control. However, in the IoT, levels of communication and collection of data are also important because the identification threat is increased due to the impact of natural interactions and emerging technologies.

B. Tracking people's location using different devices like GPS, internet traffic, and smartphone location is dangerous. Privacy violations such as user's information disclosement such as GPS tracking, disease or tracking disorder have been detected.

C. E-commerce such as advertisements and newsletters are personalized using profiling, where information is collected by organizations with the integration of data sources and other profiles. With the expansion of the IoT, data sources are exploding nowadays. Furthermore, the data quality is changed due to the increment of data collection, where the other reason is also the accumulation of individual personal life data of previously inaccessible parts.

D. Feedback to users about contacts, presentations, the number of smart items, and new ways to interact with computers. Personal information is threatened due to confidentiality between the computer and the user.

E. When the devices are in the circulation process, users use these devices more and therefore, the transitions of the life cycle occurs. Hence, all data may be destructed by that objects, where data including videos and photos of personal users are also deleted.

F. The personal items and features of end-users are accessed by gathering the information using unauthorized usage, which is known as inventory attacks. In order to destroy the property of the user, these inventory data is used by thieves to identify the safe time for that destruction.

G. While individual data sources are connected with the systems, intrusion of personal data may happen, and unauthorized access will be increased due to the linking connections between various systems [71], [72].

Apart from profiling, inventory attack and linkage, all the privacy threats have a medium level, where inventory and linkage have a low level, and profiling has a high level of threats.

VIII. DATA PRIVACY IN IOT

In the operating environment, IoT faces privacy and security as major challenges because of the various nature of large-scale devices and vulnerability. According to the report of [73], the devices of IoT are constantly increasing, where larger-scale domains are developed from small scales such as smart city is designed from smart gird by using IoT applications. However, the reputation of these IoT devices is slashed by cyber-attacks and security threats. Based on the analysis of HP, many standard IoT devices have a 25% risk per device. In the extensive security solutions, IoT trends face various issues, namely limited memory, high energy consumption and low computation processing [74]. In order to detect the physical environments, three components of IoT is used, such as sensing unit, mobile terminals and actuators, where a vast amount of sensors are presented in sensing units, and this simple architecture leads to more vulnerable threats in IoT. In addition, IoT devices are subject to various security issues and challenges. These security issues and challenges have been addressed by different authors with different approaches. In addition to providing mobile computing devices, IoT also offers software-based solutions that integrate with device security. Without human intervention, the communication between devices of IoT has occurred via machine to machine (M2M). However, mobile computing is much better because of human-machine communication. It offers hardware-based solutions, such as mobile computing, unlike IoT-based systems, computers, PDAs, smartphones, laptops, handheld devices, etc., using three components of IoT. Smartphones, laptops, and notebooks become robust and effective due to policies and procedures on security.

The application of a home automation control system is designed by using a smartphone that is paired with IoT devices, protecting these devices while the smartphone is authenticated using QR code authentication [76]. The IoT middleware is used by mobile devices, which are specifically designed for low power consumption and limited to data processing of sensitivities [77].

The security of devices is affected by mobile computing via different services, applications or infrastructure. Among the most disruptive categories of technology in the next 10 years, mobile applications and the IoT will be

connected to each other. Mobile applications can play an important role in the context of managing the IoT.

The dangers of IoT devices can be easily hacked, and mobile IoT applications can be considered to help reduce these risks, but these applications are not the same as mobile applications because of various components such as network, web and mobile in those applications. IoT requires the collection of personal information, and some serious privacy risks [80] are still faced by IoT. Nowadays, poor protection is presented in the current IoT devices, and that requires solutions for these risks such as privacy and security.

IX. FUTURE DIRECTIONS

All methods have been affected by a number of open issues so far (requiring performance, efficacy, accuracy and confidence), so future work should focus on resolving these open issues. Moreover, there are many outdated methods due to the lack of use of the latest advances in technology and methods related to privacy protection. In light of the discussion, we recommend the use of fog computing in its next work (in addition to its proximity to the client, wireless communication and data storage, filtering and processing capabilities, and collaboration between fog-to-SP transmissions). Finally, we understand the need to create a common standard framework for privacy in the IoT. We also need to focus on the privacy of smart devices.

X. CONCLUSION

In this research work, privacy, threats and their challenges are highlighted, where measures of privacy and security using privacy-preserving techniques are addressed in this study. In addition, the laws of IoT and disclosure details of privacy is also discussed, and the detailed implementation of DP with basic definitions and implementation mechanisms is provided. A systematic approach of cryptographic techniques along with privacy management is discussed, where wearable devices of IoT is used to collect the users' information and its challenges are also addressed in this work. To answer the questions that arise on the security and privacy of IoT, future directions in this area is also presented. This work will help the researchers to find useful topics on the development of IoT with high security and privacy using efficient and effective privacy-preserving techniques.

REFERENCES

[1] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, A survey on IoT security: Application areas, security threats, and solution architectures, IEEE Access, 7 (2019) 82721–82743.

[2] K. Jaiswal, S. Sobhanayak, B. K. Mohanta, and D. Jena, IoT-cloud based framework for patient's data collection in smart healthcare system using Raspberry-Pi, in Proc. IEEE Int. Conf. Elect. Comput. Technol. Appl. (ICECTA), (2017) 1–4.

[3] U. Satapathy, B. K. Mohanta, D. Jena, and S. Sobhanayak, An ECC based lightweight authentication protocol for mobile phone in smart home, in Proc. IEEE 13th Int. Conf. Ind. Inf. Syst. (ICIIS), (2018) 303–308

[4] J. Wang, Z. Cai, and J. Yu, Achieving personalised-anonymity-based content privacy for autonomous vehicles in CPS, IEEE Trans. Ind. Informat., 16(6) (2020) 4242–4251

[5] G. Xiao, G. Wang and J. Gehrke, Differential privacy via wavelet transforms, IEEE Trans. Knowl. Data Eng., 23(8) (2011) 1200–1214.

[6] M. R. Fouad, K. Elbassioni, and E. Bertino, A supermodularity-based differential privacy-preserving algorithm for data anonymization, IEEE Trans. Knowl. Data Eng., 26(7) (2014) 1591–1601.

[7] J. Soria-Comas, J. Domingo-Ferrer, D. Sanchez, and D. Megias, Individual differential privacy: A utility-preserving formulation of differential privacy guarantees, IEEE Trans. Inf. Forensics Security, 12(6) (2017) 1418–1429.

[8] H. Wang and Z. Xu, CTS-DP: Publishing correlated time-series data via differential privacy, Knowl. Based Syst, 122 (2017) 167–179.

[9] S. Goryczka and L. Xiong, A comprehensive comparison of secure multiparty additions with differential privacy, IEEE Trans. Dependable Secure Comput., 14(5) (2017) 463–477.

[10] T. Zhang and Q. Zhu, Dynamic differential privacy for ADMM-based distributed classification learning, IEEE Trans. Inf. Forensics Security, 12(1) (2017) 172–187.

[11] Y. Cao, M. Yoshikawa, Y. Xiao, and L. Xiong, Quantifying differential privacy in continuous data release under temporal correlations, IEEE Trans. Knowl. Data Eng., 31(7) (2019) 1281–1295.

[12] Q. Geng and P. Viswanath, The optimal noise-adding mechanism in differential privacy, IEEE Trans. Inf. Theory, 62(2) (2016) 925–951.

[13] Li, H. Li, H. Zhu, and M. Huang, The optimal upper bound of the number of queries for laplace mechanism under differential privacy, Inf. Sci., 503 (2019) 219–237.

[14] L. Sweeney, k-Anonymity: A model for protecting privacy, Int. J. Uncertain. Fuzz. Knowl. Based Syst. 10 (05) (2002) 557–570.

[15] J. Domingo-Ferrer, V. Torra, A critique of k-anonymity and some of its enhancements, in Availability, Reliability and Security, 2008. ARES 08. Third International Conference on, IEEE, (2008) 990–993.

[16] N. Shen, J. Yang, K. Yuan, C. Fu, C. Jia, An efficient and privacy-preserving location sharing mechanism, Comput. Stand. Inter. (2015).

[17] B.H. Bloom, Space/time trade-offs in hash coding with allowable errors, Comm. ACM 13 (7) (1970) 422–426.

[18] A.H. Celdran, F.G. Clemente, M.G. Perez, G.M. Perez, Secoman: A semantic-aware policy framework for developing privacy-preserving and context-aware smart applications, IEEE Syst. J (2014).

[19] P. Gope, T. Hwang, Untraceable sensor movement in distributed iot infrastructure, Sensor J. IEEE, 99 (2015), doi:10.1109/JSEN.2015.2441113. 1–1.

[20] P. Paillier, Public-key cryptosystems based on composite degree residuosity classes, in Advances in CryptologyEUROCRYPT99, Springer, Berlin Heidelberg, (1999) 223–238.

[21] J. Benaloh, Dense probabilistic encryption, in Proceedings of the Workshop on Selected Areas of Cryptography, (1994) 120–128.

[22] Gentry, S. Halevi, Implementing gentry fully-homomorphic encryption scheme, in Advances in Cryptology–EUROCRYPT, Springer, Berlin Heidelberg, (2011) 129–148.

[23] Z. Brakerski, V. Vaikuntanathan, Efficient fully homomorphic encryption from (standard) lwe, SIAM J. Comput. 43 (2) (2014) 831–871.

[24] J.-S. Coron, D. Naccache, M. Tibouchi, Public key compression and modulus switching for fully homomorphic encryption over the integers, in Advances in Cryptology–EUROCRYPT, Springer, Berlin Heidelberg, (2012) 446–464.

[25] J. Sen, Privacy preservation technologies in the internet of things, in Proceedings of the International Conference on Emerging Trends in Mathematics, Technology and Management, (2010) 496–504.

[26] J. Su, D. Cao, B. Zhao, X. Wang, I. You, ePASS: An expressive attribute-based signature scheme with privacy and a unforgeability guarantee for the internet of things, Future Gener. Comput. Syst. 33 (2014) 11–18.

[27] A. Alcaide, E. Palomar, J. Montero-Castillo, A. Ribagorda, Anonymous authentication for privacy-preserving iot target-driven applications, Comput. Security 37 (2013) 111–123.

[28] X.-J. Lin, L. Sun, H. Qu, Insecurity of an anonymous authentication for privacy-preserving iot target-driven applications, Comput. Security 48 (2015) 142–149.

[29] Rescorla, N. Modadugu, Datagram transport layer security version 1.2 (2012).

[30] S. Raza, Lightweight security solutions for the internet of things, Mälardalen University, Västerås, Sweden, Ph.D. thesis.

[31] M. Vucini, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, R. Guizzetti, Oscar: Object security architecture for the internet of things, Ad Hoc Netw. (2014).

[32] J. Connolly, Wearable Rehabilitative Technology for the Movement Measurement of Patients with Arthritis, Ulster University, February 2015. Available online: https://ethos.bl.uk/OrderDetails.do?did=1&uin=uk.bl.ethos.675471 (accessed on 3 August 2021).

[33] A. Pando, Wearable Health Technologies and Their Impact on the Health Industry. Forbes. 2019.

[34] Song, M.-S.; Kang, S.-G.; Lee, K.-T.; Kim, J. Wireless, Skin-Mountable EMG Sensor for Human–Machine Interface Application. Micromachines 10 (**2019)** 879.

[35] C. Massaroni, P. Saccomandi, E. Schena, Medical Smart Textiles Based on Fiber Optic Technology: An Overview, J. Funct. Biomater., 6 (**2015)** 204–221.

[36] R. Jouffroy, D. Jost, B. Prunet, Prehospital pulse oximetry: A red flag for early detection of silent hypoxemia in COVID 19 patients,Crit. Care , 24 (2020) 1–2.

[37] Best, J. Wearable technology: Covid-19 and the rise of remote clinical monitoring. BMJ 372 (2021) 413.

[38] Vijayan, V., McKelvey, N., Condell, J.; Gardiner, P.; Connolly, J. Implementing Pattern Recognition and Matching techniques to automatically detect standardized functional tests from wearable technology. In Proceedings of the 2020 31st Irish Signals and Systems Conference (ISSC), Letterkenny, Ireland, (2020) 11–12.

[39] S. Majumder, T. Mondal, M. J. Deen, Wearable Sensors for Remote Health Monitoring,Sensors, 17 (2017) 130.

[40] Cha, J.; Kim, J.; Kim, S. Hands-free user interface for AR/VR devices exploiting wearer's facial gestures using unsupervised deep learning. Sensors, 19 (2019) 4441.

[41] Sensoria Fitness: Motion and Activity Tracking Smart Clothing for Sports and Fitness. (2021).

[42] TEKSCAN. Gait Mat|HR Mat|Tekscan. Photo Courtesy of Tekscan™, Inc. Available online: www.tekscan.com/productssolutions/systems/hr-mat.

[43] Image Courtesy 5DT.com; DT Technologies Home—5DT. Available online: https://5dt.com/ (accessed on 29 July 2020).

[44] NEXGEN. NexGen Ergonomics–Products–Biometrics–Goniometers and Torsiometers. Available online: www.nexgenergo.com/ergonomics/biosensors.html (accessed on 3 August 2021).

[45] L. Cilliers, Wearable devices in healthcare: Privacy and information security issues. Health Information Management Journal. 49 (2019) 150–156.

[46] L. Tawalbeh, F. Muheidat, M. Tawalbeh, M. Quwaider, IoT Privacy and Security: Challenges and Solutions, Appl. Sci. 10 (2020) 4102.

[47] Kapoor, V., Singh, R.; Reddy, R.; Churi, P. Privacy Issues in Wearable Technology: An Intrinsic Review. In Proceedings of the International Conference on Innovative Computing and Communication (ICICC-2020), New Delhi, India, (2020) 21–23.

[48] Sankar, R., Le, X.; Lee, S., Wang, D. Protection of data confidentiality and patient privacy in medical sensor networks. In Implantable Sensor Systems for Medical Applications; Woodhead Publishing: Sawston, UK, (2013) 279–298.

[49] Alrababah, Z. Privacy and Security of Wearable Devices. (2020).

[50] Paul, G., Irvine, J. Privacy Implications of Wearable Health Devices. In Proceedings of the 7th International Conference on Security of Information and Networks, Glasgow, Scotland, UK, Association for Computing Machinery: New York, NY, USA, (2014) 9–11.

[51] Gellman, Fair Information Processing Practices, (2012).

[52] NIST (National Institute of Standards and Technology) (2014) Privacy Engineering Objectives and Risk Model. Kantara Initiative IoT workshop

[53] European Parliament and Council, General Data Protection Regulation. Official Journal of the European Union, Brussels (2016).

[54] https://iot.ieee.org/newsletter/september-2016/ [Accessed on 25th November 2020]

[55] OFCOM, Promoting investment and innovation in the Internet of Things. OFCOM, London (2015).

[56] European Parliament and Council, General Data Protection Regulation. Official Journal of the European Union, Brussels (2016). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016R0679.

[57] NIST (National Institute of Standards and Technology), NIST Big Data Interoperability Framework: 1, Definitions, Special Publication (NIST SP) - 1500-1. https://www.nist.gov/publications/nist-big-data-interoperability-framework-volume-1-definitions.

[58] Hsu, Chin-Lung, and Judy Chuan-Chuan Lin., An Empirical Examination of Consumer Adoption of Internet of Things Services: Network Externalities and Concern for Information Privacy Perspectives. Computers in Human Behavior 62 (2016) 516–527.

[59] Belanger, France, and Robert E. Crossler. 2011. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly 35 (4) (2011) 1017–1042.

[60] Culnan, Mary J., How Did They Get My Name?: An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use. MIS Quarterly 17 (1993) 341–363.

[61] Culnan, Mary J., and Pamela K. Armstrong., Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science 10 (1) (1999) 104–115.

[62] Kim, Min Sung, and Seongcheol Kim., Factors Influencing Willingness to Provide Personal Information for Personalized Recommendations. Computers in Human Behavior 88 (2018) 143–152.

[63] Xu, Heng, Tamara Dinev, Jeff Smith, and Paul Hart.., Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. Journal of the Association for Information Systems 12 (12) (2011) 1.

[64] Kelley, Patrick Gage, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. Proceedings of the SIGCHI Conference on Human factors in Computing Systems, (2010) 1573–1582. ACM.

[65] Park, Yong Jin, Scott W. Campbell, and Nojin Kwak.. Affect, Cognition and Reward: Predictors of Privacy Protection Online. Computers in Human Behavior 28 (3) (2012) 1019–1027.

[66] Kelley, Patrick Gage, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. A Nutrition Label for Privacy. Proceedings of the 5th Symposium on Usable Privacy and Security, 4. ACM, (2009).

[67] van der Werff, Lisa, Grace Fox, Ieva Masevic, Vincent C. Emeakaroha, John P. Morrison, and Theo Lynn., Building Consumer Trust in the Cloud: An Experimental Analysis of the Cloud Trust Label Approach. Journal of Cloud Computing 8 (1) (2019) 6.

[68] Fox, Grace, Colin Tonge, Theo Lynn, and John Mooney., Communicating Compliance, Developing a GDPR Privacy Label. Proceedings of the 24th Americas Conference on Information Systems (2018).

[69] ICO. Privacy Notices, Transparency and Control. A Code of Practice on Communicating Privacy Information to Individuals. (2017).

[70] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, Privacy in the Internet of Things : Threats and Challenges, Secur. Commun. Networks, (2014) 2728–2742

[71] N. Aleisa and K. Renaud, Privacy of the Internet of Things: A Systematic Literature Review,Proc. 50th Hawaii Int. Conf. Syst. Sci., (2017), doi: 10.24251/hicss.2017.717.

[72] S. Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes, and G. Zhang, IFIP Advances in Information and Communication Technology: Preface, IFIP Adv. Inf. Commun. Technol., 352 (2011), doi: 10.1007/978-3-642-20769-3.

[73] A. Dean and M. O. Agyeman, A study of the advances in IoT security, in Proc. 2nd Int. Symp. Comput. Sci. Intell. Control, (2018) 15.

[74] C.T. Li, C.-C. Lee, C.-Y. Weng, and C.-M. Chen, Towards secure authenticating of cache in the reader for RFID-based IoT systems, PeerPeer Netw. Appl., 11(1) (2018) 198–208.

[75] C.T. Li, T.-Y. Wu, C.-L. Chen, C.-C. Lee, and C.-M. Chen, An efficient user authentication and user anonymity scheme with

provably security for IoT-based medical care system, Sensors, 17(7) (2017) 1482.
[76] X. Su, Z. Wang, X. Liu, C. Choi, and D. Choi, Study to improve security for IoT smart device controller: Drawbacks and countermeasures,'' Secur. Commun. Netw., (2018) 1–14.
[77] M. Togan, B.-C. Chifor, I. Florea, and G. Gugulea, A smart-phone based privacy-preserving security framework for IoT devices, in Proc. 9th Int. Conf. Electron., Comput. Artif. Intell. (ECAI), (2017) 1–7.
[78] A. Alshahwan, Adaptive security framework in the Internet of Things (IoT) for providing mobile cloud computing, in Mobile Computing— Technology and Applications. London, U.K.: IntechOpen, (2018).
[79] W. Xi and L. Ling, Research on IoT privacy security risks, in Proc. Int. Conf. Ind. Informat.-Comput. Technol., Intell. Technol., Ind. Inf. Integr. (ICIICII), (2016) 259–262.
[80] R. Romaen-Castro, J. López, and S. Gritzalis, Evolution and trends in IoT security, Computer, 51(7) (2018) 16–25.