An exploration of the Wearable Internet of Things (WIoT) Users' Privacy Concerns in healthcare domain

Rawan Alharbi, Haya Almagwashi

Abstract*: Internet of things (IoT) is earning a significant role in the health care domain. Though the growing benefits to improve the health process and services and the large use of the Wearable Internet of Things (WIoT) devices, the patient's privacy issue remains a big concern. While IoT devices and its applications are more exposed to privacy risks, there is a need for a stick and strict guidelines and solutions to assist and solve this issue and minimize these risks. The aim of this paper is to survey the end-user concerns of the privacy issues related to WIoT then we review conducted on current solutions that are worked toward preserving privacy in the healthcare domain, and finally, we state our solution. This paper aims to survey end users' privacy and security concerns and issues related to WIoT.

Keywords: Internet of Things (IoT); preserving-privacy; Wearable IoT; Privacy; differential privacy

I. INTRODUCTION

The concept IoT defined as connected devices through network with mainly physical aims (e.g. sensing, heating/cooling, lighting) through interoperable protocols, often added to these systems [1]. The primary aim of IoT is to guarantee better communication between objects and establish a sustained bond among them using different types of applications [2]. IoT research covers many various areas and engage with different research scopes, starting from enabling technologies (e.g. sensors, protocols, networks), software architecture (e.g. middleware, cloud solutions, data management, big data), services and applications (e.g. smart homes, smart cities, connected cars), social impacts of the IoT (e.g. acceptance of users, change in the societal organizations, change in control of the infrastructure). Wearable technology is mostly defined as one of the greatest applications of the Internet of Things. Wearable electronics that individuals can wear it on their bodies have the potential to transform the way we live. Devices such as Fitbit Charge from Fitbit and Apple watch from apple company [3] enable the individuals to track their health and exercise progress in a way that were impossible before. The sensors can today be added to anything such as our clothes, watches, glasses etc., capturing the daily human's behavior and creating a sensitive source of data. While the power of this trend is huge the adoption, scale and development of IoT are hindered because of several challenges. These include privacy and security concerns, limited hardware capabilities, software and firmware issues, public acceptance etc. The gathered data includes a heartbeat, temperature and humidity level till the location of the wearer himself and his living habits. As such, privacy concerns raised. Also, because of the data these devices can collect and store, today IoT devices are major goal for attackers looking to obtain this data. Further, given the always on network connectivity some of these devices hold and the several usage pattern, these devices could be affected by malware, with big chance for harmful usage. Therefore, like each new technology, the IoT brings with its benefit's new concerns. One of these concerns in WIoT is how Quickly WIoT devices are being engaged to our surroundings and how much of sensitive and private data have been collected through these devices. The IoT is changing the way people work, live, and play, and societies around the globe are gaining a greater ability to control their environments to suit their personal needs and preferences while at the same time these devices are collecting personal data about its users which violate their privacy. The IoT has released a huge amount of data available, related not only to users as in tradition internet, but to many in general, groups, and organizations. This can be misused for determine what we are interested in, where we go, and our intentions. Whilst this can offer big chances for improved services, it must consider our privacy concerns. It is vital that consumers trust the services they engage with or devices that they wear it to guarantee their privacy. Trust is an essential item in the forming of any relationship and is a main factor in the acceptance of WIoT technology [4]. It is agreed that privacy is a serious concern in (WIoT) [5], along with the need of awareness by the public of the restricted data security related WIoT. those WIoT applications can cover the simple light bulbs and smart plugs that can remotely turn on a coffee machine or crockpot, to more sophisticated devices like Smart TVs and wearable technology [6]. There is limited body of research's regarding IoT privacy requirements with few studies investigated the security requirements of IoT devices to help enhance the security inside these devices. Exploring security and privacy requirements in advanced applications, such as the WIoT systems, is needed in safeguard against failures and offer wider individual acceptance.

Revised Manuscript Received on June 22, 2020.
***** Correspondence Author
Rawan Alharbi*, Department of Computer Information Systems, King Abdul-Aziz University, Faculty of Computing and Information Technology, Jeddah, Saudi Arabia.E-mail: ralharbi0447@stu.kau.edu.sa
Haya Almaguwashi, Department of Computer Information Systems, King Abdul-Aziz University, Faculty of Computing and Information Technology, Jeddah, Saudi Arabia.E-mail: halmagwashi@kau.edu.sa

II. IOT PRIVACY REQUIREMENTS

After investigating many privacy enhancing technologies, principles and the accumulation of privacy requirements for WIoT in the medical domain in previous research [21], we summarized it below and show associate efforts in privacy preservation laws and guidelines that cover it as in table 1:

TABLE I. Summary of the privacy requirements

Requirements	Regulations & law [21]
1. Users control over their data & User participation	▪ HIPPA ▪ Alliance for Internet of Things Innovation (AIOTI)
2. Privacy Enforcement	HIPPA
3. Anonymization or Pseudonymization	▪ PET ▪ AIOTI ▪ City of New York (NYC) Guidelines for the Internet of Things
4. Personal Data Protection	PET
5. Partial Data Disclosure	PET
6. Lawfulness & transparency	▪ GDPR ▪ European Union Agency for Network and Information Security (ENISA)
7. Purpose limitation & limit the PII processing	GDPR
8. Data minimization	GDPR
9. Accuracy	GDPR
10. Storage limitation	GDPR
11. Confidentiality	▪ GDPR ▪ CableLabs - A Vision for Secure IoT ▪ ENISA
12. Accountability &Risk Impact Assessment by Design	▪ GDPR & ▪ AIOTI
13. The right to access, copy, and inspect a patient's PHI	HIPPA
14. The right to request the correction of inaccurate health information	HIPPA
15. The right to request confidential communications means for PHI	HIPPA
16. The right to file complaints	HIPPA
17. Protect data security	NISTIR 8228
18. Unlinkability	PET
19. Unobservability	Broadband Internet Technical Advisory Group (BITAG)
20. Simplicity	PET
21. Authentication & authorization	(ENISA)
22. Strict user privacy preferences	▪ ENISA ▪ Online Trust Alliance (OTA)
23. Secure storage capability	▪ TR-0008-V2.0.1 Security (Technical Report) ▪ Online Trust Alliance (OTA)
24. User-Centric	- (AIOTI) - Report: Working Group 4 – Policy
25. Data Sovereignty for cloud data storage	▪ GDPR ▪ Object Management Group (OMG) Cloud Standards Customer Council (CSCC) [21].

III. SURVEY ON WIOT DEVICES USAGE IN HEALTHCARE DOMAIN

If In order to study the user concerns about their personal data privacy while using WIoT, we developed the following hypothesis based on the collected requirements on the previous section. These hypotheses are listed below:

1. People are willing to use WIoT that collect their private health information despite having concerns about their privacy.
2. People would like to have control over their collected personal health information when using WIoT in healthcare.
3. People prefer to apply control over their privacy preferences through the WIoT devices.
4. People would like to know how their personal health information is used when collected via the WIoT.
5. Preserving privacy of the users of WIoT devices will increase their acceptance of using these devices in the healthcare domain.
6. People would like to ensure that PHI (Personal Health Information) via WIoT is accurate and up to date.

A survey to test the above hypotheses was conducted to get information and feedback about the end users & patient's opinions and their privacy requirements when using WIoT devices and to help understand their level of concerns about their personal privacy and their attitude according to that.

The survey focused on end user which are the patients or regular wearers of the WIoT and their wellness to use these devices for medical proposes.

The target audience were WIoT users who speaks Arabic or English from both gender and of age 18 and above, healthcare providers and end users whether patients or wearers of wearable internet of things devices.

Due to the large sample population, the convenience sampling technique was used. It is a kind of non-probability sampling process where the sample is taken from a group of individuals easy to contact or to reach them [20]. The survey distributed to the targeted audience online through formal email, and to some of medical communities and groups social media groups such as: Twitter, WhatsApp & LinkedIn technical groups and received 200 responses were received.

A. Survey Results:

1. Demographic information:

The participants where between 30-39 year with 51.8%, to 40.2% between 18-29 year and the rest with 7.1% their age where 40-59 year. For the gender most of them where male with 67% while 33.9% where female. And about 54.5% of the participants education level is Bachelor's degree while 33.9% are holding Post graduate degree and 10% level of education where between High School and Diploma after High school.

2. Information about the use of wearable Internet of things devices and user privacy:

Of all the participants, 33% do not intend or use WIoT devices while 29.9% of the participants are willing to use WIoT devices for healthcare and 22.3% of the participants use the WIoT devices for general purposes while 10.10% are users of WIoT devices for healthcare purposes.

B. Findings:

From the analysis of the survey results, the research came out with the following findings which summarize the result as below:

- 56% of the participants have concerns about their privacy when using WIoT devices.
- Of all participants, (90%) think that WIoT service providers must take extra steps to ensure that the PI in their files is accurate and transmitted in secure way.
- Of all users, (74%) agree that the protection of their personal information in their daily life is less when they are using WIoT devices.
- Nearly over two thirds of the users (69%) believe that they have enough information about how new technologies can affect their personal privacy and they have sufficient knowledge about their privacy rights
- Half of the participants (50%) think that they can control how their personal information is collected and used by organizations.
- 45% of the participants think that the growth in technology increased their concerns about leaking information about their body.
- Over half of the participants (52%) agree on collecting data about them for medical purposes but equally (70%) they are requesting to know the purpose of collecting data about them through WIoT devices and to use and disclose their medical information after anonymizing their identity and those data should not be shared with third party unless specifically authorized to do by user.
- Of all participants (67%) think that the service providers should handle their information responsibly and they should be provided with control over their privacy via WIoT devices.
- About (45) of the participants have concerns if someone gaining unauthorized access to an internet-connected medical device such as a pacemaker belonging to the wearers.
- 52% of the participants think that the use of WIoT devices will increased if a default specific privacy preference is provided to protects the user's privacy.
- Of all participants (57%) think that should be a clear procedure provided by the service provider to correct errors in the personal information and allow them to request modification on their data.

C. Discussion:

Hypothesis 1: was rejected most of the participants have concerned about their privacy when using WIoT devices and that the growth in technology increased their concerns about leaking information about their body and this cover the purpose limitation & limit the personally identifiable information processing, processing, Personal Data Protection, Users control over their data & User participation, Data minimization, Confidentiality and Secure storage capability requirements.

Hypothesis 2: Results proved that users are aware of how much this device can affect their privacy and what is their privacy right. Participants think they can control how their personal information is collected and used by organizations which prove the need to provide them with control over their collected personal health information when using WIoT in healthcare that mentioned on this hypothesis and can be linked the identified privacy requirements: Anonymization or Pseudonymization and Partial Data Disclosure.

Hypothesis 3: This was proved as the results show that users are willing to use of WIoT devices if a default specific privacy preference is provided to protect the user's privacy. This can be linked to the identified Authentication & authorization and Anonymization or Pseudonymization requirements.

Hypothesis 4:As mentioned in hypothesis 4 and 2 results proved that most of the participants support collecting data about them for medical purposes but they are requesting to know the purpose of collecting data about them through WIoT devices and to use and disclose their medical information after anonymizing their identity and those data should not share with third party unless specifically authorized to do by user. This can be linked to the identified requirements relevant to providing users to control over their data & User participation, Anonymization or Pseudonymization, Purpose limitation & limit the PII processing and Data minimization requirements.

Hypothesis 5: The survey results show that participants believe that the service providers of the WIoT in healthcare should handle their information responsibly, and the regulators should ensure privacy standards towards the personal data and the manufacturers should provide the users with control over their privacy via WIoT devices which will lead to increase the acceptance of their use. This is relevant to the following privacy requirements: Accountability & Risk Impact Assessment by Design, Enforcement, the right to request confidential communications means for PHI, the right to file complaints, Protect data security and Confidentiality requirements. Users feel the protection of their personal information in their daily life is less when they are using WIoT devices and that decreased their willing to use it while of their privacy was preserved, their acceptance of using these devices in the healthcare domain will increase. Hypothesis 6: The survey results support this hypothesis as more users think that service providers must take extra steps to ensure that the PI in their files is accurate and the send over secure way and should provide a clear procedure to correct errors in the personal information. This covers the privacy requirements of accuracy, the right to access, copy, and inspect a patient's PHI and the right to request the correction of inaccurate health information requirements.

D. Privacy Requirements

Below the previously identified privacy requirements listed based on the survey results and prioritized based in the participants responses:

Table- II: Privacy requirements ordered based on the results

Importance in %	Requirement
1.	Anonymization or Pseudonymization
2.	Confidentiality
3.	Personal Data Protection
4.	Partial Data Disclosure
5.	Purpose limitation & limit the PII processing
6.	Data minimization
7.	Users control over their data & User participation
8.	The right to file complaints & Enforcement
9.	Authentication & authorization
10.	Accuracy
11.	The right to access, copy, and inspect a patient's PHI
12.	The right to request the correction of inaccurate health information
13.	Accountability & Risk Impact Assessment by Design
14.	Secure storage capability

After investigating user's privacy concerns when using WIoT and their privacy requirements, we surveyed existing privacy preservation solutions for IoT against the identified requirements.

IV. RELATED WORK

Before Many solutions have been proposed to enhance the privacy of the WIoT devices (WIoT) in the domain of the healthcare. Some of these solutions focused on developing frameworks from different point of view and another design model to increase the privacy related to the wearable of IoT systems, devices or applications. Few of these researches studied the privacy requirements and took it into consideration while developing their solutions. Below review of the current privacy efforts from many aspects, however, we need first to identify the meaning of private data from different perspectives:

A. Private Data:

General Data Protection Regulation (GDPR) [2] defined personal data as "any information relating to an identified or identifiable natural person" and this covers both direct and indirect identification. The identification can be as any unique number or to one or more factors related to the person such as his physical, physiological, mental, economic, cultural or social identity". However, there is no one privacy definition yet that is able to cover all the various elements of privacy, but there are guidelines that list the current identifiers to help in identify any person from other [6] and we list some here:

- Names, Location, Dates (other than year)
- Phone & Fax Numbers
- Electronic mail addresses
- Social Security, Medical Record & Health plan beneficiary numbers.
- Account & Certificate/license numbers
- Vehicle license
- Web Uniform Resource Locators (URLs) & Internet Protocol (IP)
- Biometric prove
- Photographic images
- Any other unique identifying number, characteristic or code.
- In fact, above list of PII is not comprehensive, as technology growth and newer PII might appears [6].

B. Privacy Frameworks and Solutions:

Privacy of the Internet of things devices in healthcare from the side of consumers' privacy remains a debatable issue. Study stated that there's rise in terms of awareness amongst patients where data privacy is concerned. While IoT based medical applications are more likely to face privacy concerns and risk, this drive the need to review the general privacy guidelines for health applications and enhance it to support the individual health information privacy. In this matter a compliance scale modelling the privacy principles for privacy-aware novel IoT-based health applications was proposed [9]. An analytical review of privacy guidelines was conducted to summarize the main principles and requirements to develop and evaluate a privacy aware IoT health applications with focus on only relevant principles and guidelines. After the analytical review, a quantitative survey was distributed to assess the suggested scale and conclude the principles based on their importance.

The suggested compliance scale introduces fundamental privacy principles to stick in the developments of IoT healthcare applications and are more important especially for the policymakers and applications developers to comply with and respect the privacy principles of individuals towards novel IoT-based health applications. The outcomes show that the access control, anonymity, consent, data disclosure, data minimization, openness and transparency, purpose of specifications, and safeguard and remedies are fundamentals requirements to be take in consideration while developing a privacy-aware health application. The extracted principles make up a standard that will be useful for policymakers and applications providers to recognize and apply the privacy requirements of individuals towards IoT-based healthcare systems. Compliance scale still not tested using actual IoT health applications and there is a need to validate the actual framework with real-world IoT applications [9].From another aspect, a study discussed privacy concerns in sensor networks [10]. Today sensor-based networks became a truly available anywhere technology that had influence the lives of the people in their life. While those technology offering chance for advanced, conditions-aware services, at the same time sensor networks rise privacy risks. In this study, the authors focus on determining the requirements for privacy preserving deployments. The study also reported a set of requirements to design privacy aware sensor networks. It suggested a framework that was derived based on the comprehension built on privacy requirements and obstacles in preserving privacy. The framework identifies five principles that are focused on sensor networks, which is the basis to improve global IoT-based solutions that are known to increase huge privacy risks. This framework aimed in determining the requirements for designing a privacy aware network but even when it is an IoT framework, the attention is into security requirements which may not be suitable for IoT healthcare applications in common. As there is an issue raised in differentiating between privacy and security principles at the time that both are related to unlike aspects [10].On another hand, IoT is developing to be a more loosely coupled decentralized system of collaborative smart things in term that support rapid speed data processing and analytics with short response time. The dementalization has big effect on the way individual information generated and used by smart objects. However, this raise the need for more protection measures because without centralized data management its harder to monitor and control how data linked and used by these smart things. A framework [8] was proposed to allow WIoT user to choose and specify their privacy preferences and a compliance check of user individual privacy preferences is carried immediately by smart objects, rather than by a central object. The research focused on designing a decentralized privacy enforcement mechanism. The proposed privacy preference model designed with group of privacy metadata which used with smart things for check and implement individual privacy preference at smart object level. As a result, smart things can derive the meta-data for recently created items. Following the operations executed over the data, smart things examine the implementation of the privacy laws of the user‘s data with the privacy choices related to these data item [8].Another recent study [11], has introduced a framework identifying seven principles concerning the privacy of disabled users. These are as follow:

1. Users must know who owns their medical data.
2. Patients acceptance for handling their health data.
3. Pseudonymity to anonymize Patients PII by means of separating the identity of a patients.
4. Hide patients Location.
5. Maximizing the locality of information.
6. Privacy for IoT devices.
7. Considering privacy from the first stage of the application design.

These seven principles considered as privacy requirements for IoT applications for disabled users in healthcare domain that must be followed to ensure their privacy. This study differentiates clearly between privacy and security requirements by different principles. The study mainly focused on the privacy requirements for the disabled user which are not relevant for IoT health apps in general. The framework lack essential principles such as protection of ownership of consumers' health information [11]. Guidelines for protecting privacy in IoT in general were proposed by [12]. These guidelines introduced are usable to control the privacy concerns of several areas exactly for medical, smart houses and supply management. It offers insight about the privacy requirements that demands to be merged in the development of privacy frameworks for WIoT- medical systems. The guidelines developed are based on checking the complementary pieces of technology privacy frameworks and the IoT network attributes such as the technological aspects and legal regulations. The proposed solution offers nine features to be added when deploying an IoT privacy framework.The framework is general as it provides the features that must be added when developing an WIoT privacy framework that can be applicable and helpful to design various types of IoT health applications. The framework principles are rather ambiguous and has overlapping with each other's such as identity privacy, query privacy, temporal and location privacy that could be combined together under one principle named user anonymity [12].Patients' safeguarding of healthcare data are major issues that will have an effect on the coming achievement of Healthcare with IoT. The main issue in the use of IoT for healthcare systems is enhancing privacy. The high dependencies between health care systems is a huge problem to achieve users' privacy as healthcare service provider systems collect data from wearers and share it with medicals experts. Those providers also, might probably share the data to pharmaceutical companies and health insurance companies [12].To solve the issue, Dwivedi in [13] proposed privacy-preserving scheme with important data extraction from IoT devices linked with healthcare systems. Based on the proposed scheme, the data collected from WIoT devices is handled for safeguard the critical data, such that unknown people are locked from accessing them using Ml algorithms. Grey Wolf Optimization (GWO) scheme is presented to identify the optimal key. The scheme aimed to reduce hiding failure rate, modification degree, and true positive value for better preservation of critical data.

The applied solution featured with conventional schemes like Genetic Algorithm (GA) and other in level of performance [13].Remote patient monitoring WIoT devices systems raised pose grave privacy risks in term of data transfer and the logging of data transfers. Those a privacy issues of healthcare database might cause a delay in treatment progress. A study by Luo [14], suggests applying blockchains to conduct secure management and examination of healthcare big data. Blockchains are pricy and need high bandwidth and not suitable for most of the IoT devices. In this matter, a novel framework of adjusted blockchains models suitable for IoT devices that depends on their distributed mechanism and further privacy properties of the network. The privacy and security properties in the framework depends on advanced cryptographic primitives which make the data transmission over the IoT healthcare system more secure and anonymous using a blockchain-based network. The solution offers a combined approach of the private key, public key, blockchain and more other to design a patient-centric access control for electronic medical records, with ability to safeguard the security and privacy [14].In IoT medical devices are more at risk to many security threats. Many solutions developed to provide protection to patients' data during data transmission but unfortunately these solutions are unable to prevent risky attacks such as collusion attacks and data leakage and cannot safeguard the patient privacy. A practical framework named PrivacyProtector [15] was proposed for protecting patient's privacy at the data collection, seeking to prevent the attacks. PrivacyProtector contains the concept of strictly confidential sharing and share Fixing for healthcare PII privacy. The framework uses the Sle- pian-Wolf-coding-based secret sharing (SW-SSS) in PrivacyProtector with distributed database that contains many cloud servers to safeguard that the PII of patients will be protected for long period of time without revealing the PII. The performance test display that the PrivacyProtector framework is preserving the privacy versus various attacks [15].For the healthcare information systems (HISs) that used IoT wearable technology, privacy became a significant issue in the term of safeguarding patients' personal data. Some privacy enhanced healthcare information frameworks were proposed. The authors in [16] presented a privacy-preserved healthcare information system framework and explore the role of privacy protection in HISs. It provided modules for designing, privacy safeguard, access control, and secure transmission to improve the privacy safeguard of healthcare information systems. The paper presented an example of the implementation of the proposed framework as a test of privacy-preserved systems. The framework focuses on the consideration of the general opinion of acceptance and usage of technology to study the individual acceptance of a privacy-guaranteed systems. The investigation outcomes proved that the individual acceptance of these systems is directly affected by social impact, performance expectancy, ease conditions, and awareness of security [16]. In another study [17], a privacy preserved medical system is suggested to safeguard the sensitive data of an users also to discover vocal disorders. The mechanism of the designed medical system is based on the suggested zero-watermarking algorithm, which adds a watermark to a secret key as an alternative of the signals to avoid the change in a voice pattern. The sensitive data is protected by the generation of its secret shares over visible cryptography.] The suggested solution is tested through using voices patterns from voice disorder database. Test outcomes show that the offered solution fulfill imperceptibility [17].One One of the uses of the internet of things in the medical area is by using machine learning technology to handle the data that contributed to medical IoT for health examination and illness detection. Data analysis and information on medical issues detection might expose personal private information. Proper handling of this critical medical information is needed to avoid unauthorized linkage to individuals and the jeopardizing of their privacy. To offer privacy-preserving cluster inquiry in medical IoT, Efficient Differentially Private Data Clustering Scheme (EDPDCS) based on MapReduce framework was suggested [7]. In EDPDCS, the authors optimize the allocation of privacy budgets and the selection of initial centroids to enhance the accuracy of differentially private K-means clustering algorithm. In addition, an improved initial centroids selection method is suggested to maximize the accuracy of the clustering algorithm. Finally, they show that the suggested EDPDCS can increase the accuracy of the differentially private k-means algorithm through comparing the Normalized Intra-Cluster Variance (NICV) produced by their algorithm with other 2 datasets. The proposed solution tested on 2 group data sets that contain personal information related to medical domain, the algorithm EDPDCS successed in NICV and enhance the accuracy of the clustering outcomes while safeguard individual data [7].

V. PROPOSED APPROACH

WIoT is gaining a big rule in the healthcare domain. Though the growing benefits to improve the health operation and the great use of the WIoT devices, the patient's privacy issue remains a big concern. While growth of data leaks, attacks, and other malicious software in the last couple of years have noted out concerns about data security and privacy. All this negatively affect the sharing and spreading of data. To address these many issues, enhancing techniques and solutions are needed for preserving data.

Privacy-preserving ML has given large-scale research in the context of data transformation and analysis. So, it is of great attention to look whether the present solutions can be put in the context of IoT.

Machine learning data Transmission-Based Approaches: is a category of approaches which allows participants to send local data samples to the third party, while protects certain aspect or attribute of the data samples, e.g., user identity, data contents, or raw from the data. It has the following sub-categories: anonymization, cryptographic methods, data obfuscation, and data synthesis [19].

Anonymization techniques are designed to anonymize the end user who is the patient's identity in a group of users, changing the value of identifiers and removing clear identifiers. Since the goal is to remove the bond between data entries and the data owner, the data samples of interest used for model training remains unchanged. For field-structured data, anonymization techniques include k -anonymity, l -diversity, and t -closeness [19].

Based on above review, the proposed solution will be implemented on a set of ML algorithms for achieving privacy preservation for data extracted form WIoT through using differential privacy hyper parameter on healthcare dataset and compare their accuracy and performance. Differential privacy Offers solid numerical evidence for privacy preservation. The goal of this technique is to increase query accuracy and decrease the likelihood of privacy leakage. Differential privacy can be achieved through adding randomization noise to the query outcomes to safeguard individual entries without major change in query outcomes [19].

Our method consists of four main steps which are: Feature extraction, data cleaning & pre-processing, splitting Data and implementation of machine learning algorithms with DP. Below description of each step:

- Feature Extraction: Anaconda using jupyter open source used to import and explore the data in readable format. It reads the CSV file and produces a visual document of the features extracted, and also offers a csv file of the dataset.
- Data cleaning & pre-processing: cleaning and Pre-processing data process is regular step are used to clean the data from the null and non-useful value and transform it into a suitable form for machine learning. It includes cleaning the dataset by removing irrelevant or corrupted data that can affect the accuracy of the dataset.
- Splitting Data: During the machine learning process, two type of data are needed one for training and other for testing and evaluation. In our research, we considered 80% of the patient's dataset to be the training data and the remaining 20% to be the testing data.
- Implementation of Machine Learning Algorithms with DP: All the experiments were done in Python 3.4 by relying on Python machine learning libraries (diffprivlib, Mat- plotlib, Pandas, and NumPy).

In this context, the 5 algorithms used to examine with differential privacy hyper parameter is Naive Bayes (NB), Logistic regression, Linear regression, K-mean (K-mean) and Principal component analysis (PCA).

VI. CONCLUSION

The advance growth of WIoT devices industry led to a vast revolution on many areas such as education, smart cities, healthcare, etc. These technologies used nowadays linked as WIoT to collect and exchange data to improve the end user's health life or to provide them with several customized services. However, the privacy of individual data is still a critical issue that must be handled in depth. This is a significant requirement where sensitive data is being used such as in Healthcare or other areas. A survey was conducted and has shown that there are many concerns on this regard. Based on the survey results and investigation of relevant literature, a list of privacy requirements has been identified. Recent privacy enhancing frameworks and solutions have been discussed, however, there is still a need for a comprehensive solution that covers most if not all the identified privacy requirements. The paper proposed privacy enhancing approach that use ML and differential privacy algorithm to preserve the privacy while analyzing the data. The future research will investigate many machine learning algorithms after adding noise using differential privacy then evaluate the privacy loss and the accuracy. Differential privacy provide mathematical proof of preserving the privacy while perform different kind of data analysis.

REFERENCES

1. R. Farzad Kamrani, Mikael Wedlin, "Internet of Things: Security and Privacy Issues," 2017.
2. M. B. Yassein, M. Q. Shatnawi, D. Al-zoubi, and 2016 International Conference on Engineering & M I S (ICEMIS), "Application layer protocols for the Internet of Things: A survey," pp. 1–4, 2016.
3. S. Kumar, "Technological and business perspective of wearable technology.," 2017.
4. C. Maple, "Security and privacy in the internet of things," J. Cyber Policy J. Cyber Policy, vol. 2, no. 2, pp. 155–184, 2017.
5. O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and Security in Internet of Things and Wearable Devices," IEEE Trans. Multi-Scale Comp. Syst. IEEE Trans. Multi-Scale Comput. Syst., vol. 1, no. 2, pp. 99–109, 2015.
6. M. UGUR, Naciye. BARUTCU, "A Critical analysis on Internet of Things: Features and vulnerabilities. Sakarya University.," 2018.
7. Z. Guan, Z. Lv, X. Du, L. Wu, M. Guizani, "Achieving data utility-privacy tradeoff in Internet of medical things: A machine learning approach", Future Gener. Comput. Syst., vol. 98, pp. 60-68, Sep. 2019.
8. Sagirlar, G., Carminati, B., & Ferrari, E. (2018). Decentralizing privacy enforcement for Internet of Things smart objects. Computer Networks, 143, 112–125. doi:10.1016/j.comnet.2018.07.019
9. Aivaloglou, E., Gritzalis, S., & Skianis, C. Requirements and Challenges in the Design of Privacy-aware Sensor Networks. Retrieved from http://ieeexplore.ieee.org/document/4150864/. 2006.
10. Al-mawee, W. Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users a Survey. Retrieved from http://scholarworks.wmich.edu/cgi/viewcontent.cgi?article=1661&context=masters_theses . 2012
11. Ruback, T. (2015). Understanding the Differences Between Privacy and Security Online. Retrieved from https://www.ghostery.com/intelligence/business-blog/privacy/understanding-thedifferences-between-privacy-and-/
12. Comparative Assessment on Privacy Preservation in Health Care Sectors coupled with IoT
13. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. Sensors 2019, 19, 326.
14. E. Luo et al., "PrivacyProtector: Privacy-protected patient data collection in IoT-based healthcare systems", IEEE Commun. Mag., vol. 56, no. 2, pp. 163-168, Feb. 2018.
15. Hsu, C. L., Lee, M. R., and Su, C. H., The role of privacy protection in healthcare information systems adoption. *J Med Sys* 37(5):9966, 2013. doi:10.1007/s10916-013-9966-z.
16. Logrippo, Luigi. Abdelouadoud, Stambouli. "Configuring Data Flows in the Internet of Things for Security and Privacy Requirements". 2019. DOI: 10.1007/978-3-030-18419-3_8
17. Alsamiri1, Jadel. Alsubhi, Khaled. Internet of Things Cyber Attacks Detection using Machine Learning. International Journal of Advanced Computer Science and Applications, Vol. 10, No. 12, 2019
18. Zheng, Mengyao. Jiang, Linshan. Challenges of Privacy-Preserving Machine Learning in IoT. 2019.
19. M. Du, K. Wang, Y. Chen, X. Wang and Y. Sun, "Big Data Privacy Preserving in Multi-Access Edge Computing for Heterogeneous Internet of Things," in IEEE Communications Magazine, vol. 56, no. 8, pp. 62-67, August 2018.
20. Homas W. Edgar, David O. Manz, in Research Methods for Cyber Security, 2017.
21. Alharbi, Rawan. Almagwashi, Haya. The Privacy requirments for wearable IoT devices in healthcare domain. 2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW). 2019

AUTHORS PROFILE

Rawan Alharbi is an Ecommerce & Ebanking Support officer at Arab national bank, Saudi Arabia. She had her BSc degree with honors in Computer Information System from King Abdul-Aziz University, Saudi Arabia, in 2016. She has an MSc in computer information system- IoT privacy & security from King Abdul-Aziz University, Saudi Arabia. Rawan research interests include IoT privacy in healthcare domain. She has published several publications in peer- reviewed journals and conference.

Haya almagwashi is Assistant Professor, Department of Information Systems, Faculty of Computing and Information Technology, King Abdul-Aziz University, Jeddah, majoring in information security and privacy. She received her BSc degree from Computer Science Department, College of Science, King Abdul-Aziz University, Jeddah, Saudi Arabia. She completed her MSc degree from Computer and Information Sciences, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. She received her PhD degree from Computer Science and Informatics, College of Computer Science and Informatics, Cardiff, United Kingdom. Her research interests include information security strategies for organizations, maintaining privacy in e-government services, and IoT security.