NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 5, ISSUE 10, Oct.-2018

IOT AND THE ISSUE OF DATA PRIVACY

Ashok Kumar Reddy Nadikattu
Sr. Data Scientist & Department of Information Technology
California USA

ABSTRACT
Internet of Things (IoT) can revolutionize the way people live in various sectors that deal with connected devices such as entrainment, businesses, and the government. IoT is a crucial area that most Research needs to be done on as it gives an idea on the intelligent collaboration of devices can be experienced anywhere and anytime. IoT poses some concerns that make people question its adaptability, and some of the challenges may include data privacy and security. The speed of the growth in devices that need IoT is high, meaning it's something that has a significant impact on issues on data privacy. The research paper discusses how IoT relates to security and issues in data privacy. It also highlights what the prevalent security threats are in layers of IoT. The Research will be essential to the users in the world and the United States as they can learn how they can make IoT secure and easily adoptable to ensure their devices are protected from malpractices or access to private data from unauthorized people.

KEYWORDs: Internet of Things (IoT), Privacy, Security, Data Privacy, and Access Control

INTRODUCTION
The Internet of Things is often compared to a nervous system or electricity for the planet that defines unseen and pervasive phenomena and can be integrated into the community. Generally, IoT is the networking of physical objects which can connect through the Internet. For many years, devices have been communicating to each other, making the Internet of things not to be classified as a new concept. The difference can be on how various sensors more sophisticated nowadays; Big Data analytics and cloud are computing are available for companies to store information and how IoT computing devices are more accessible and affordable. Data protection, businesses, and government authorities in the world are trying to anticipate the impacts of using the Internet of things regarding data privacy for a good reason (Frustaci et al., 2017). The profound economic, social, and political transformations of surveillance and privacy are essential in connecting IoT and the issue of data privacy. Thus, this can take ideas from all the Internet of Things-related projects to show what it will bring to data privacy.So far, several observations have been made concerning the matter, and it gives the direction to what can be expected as the outcome of the relationship. Sensor data are high in sensitivity, quality, and quantity; hence, it makes it easier for the Internet of things to gather personal data. The value is not on the devices the business uses for data privacy but on the new services concerning IoT and the information they can combine and amass. IoT challenges are also considered to ensure privacy is not breached; it can be a trusted technology idea.Targeting, tracking, and profiling groups of people are expected to be accurate, specific, and nuanced to ensure the Internet of Things does not alter company data privacy. Thus, if a device becomes connected to the company, it can be easy for them to mine and track the behavior patterns. The data generated by the devices can now be known, and contiguous information may be revealed to the public, which is not as per the company's wish. It conveys essential information about privacy risks, and it becomes a challenge to the users. With this regard, it is vital to discuss how IoT can be involved in data privacy and how such information from the Research will help individuals from the United States.

LITERATURE REVIEW
IOT AND THE ISSUE OF DATA PRIVACY
The development of the Internet of things among organizations means that they are ready to preserve privacy. It involves adopting data security and privacy by collecting consumer data indicating the consumer consent of data privacy and how they can access the data. Protecting consumer privacy is somehow tricky for IoT as it is more prevalent (Punia et al., 2017). The connection of more devices leads to less control as the control of devices and data control are connected at stake. If someone hacks the devices, control can be lost, making it difficult for IoT to ensure the privacy of information shown to the public. Control can also be lost when the

companies are gathering user's information (Ali et al., 2017). It may make the organization alter with the privacy policies, which affects the Internet of Things, which is responsible for ensuring data privacy is maintained as IoT cannot get the control over such data lost.

The Internet of things devices is connected to the Internet, making them vulnerable to cyber-attacks that affect other computer systems. Thus, this proves weak security with regards to the Internet of things as data privacy cannot be maintained. IoT devices' idea of connectivity to function makes hackers access such devices as they have a common attack vector that is easier for hackers to crack (Terry, 2017). The difficulty in patching Internet of things devices makes the security flaws to be hardly unaddressed, proving that the issue of data privacy is not handled well. In cloud services, some risks are posed by IoT, which makes the chances of data being compromised and splitting control to other devices, which makes it hard for users to limit access to their data (Banafa, 2017). The consistent security now depends on harmonizing data security practices that use the Internet of things to transmit, collect, and store secured data. IoT functions on various devices make it clear that an organization weak cybersecurity is the root of serious impacts such as hacking, injury, and physical damages. Device heterogeneity, identification, and authentication are the primary privacy and security concerns surrounding the Internet of things. The concerns relate to the challenges: surveillance, business models, ethics communication mechanism, scalability, and integration. IoT has spread in most parts of the world (Chernyshev et al., 2017). The organizations are expected to better their privacy and security protection, making their devices vulnerable to data breaches and corporate surveillance that may need to access the information linked to the consumers, making data privacy issues increase. The most challenging part of the Internet of Things is that it makes the consumers surrender their privacy slowly as they are not aware of how the data is being collected, how it will be used, and what data is collected. The authentication and identification process can now be altered, putting the organization at high risk of losing such consumers (Javed et al., 2017). When such things occur to the consumer, their devices will be easily monitored. Ethics communication mechanism will not be considered the blame will be placed on IoT, which has failed to maintain and track the steps to ensure data privacy is maintained.

The IoT manufacturers can be linked to a lack of compliance that brings about data privacy issues under the Internet of things. It is the most significant security issue with IoT as the manufacturers create devices that have poor security, and the Internet of things cannot protect them (Daud et al., 2017). The users can also be blamed for such things since they are not always keen and aware of the functionality of IoT when they purchase any device. They give the hackers the space to control their products reduce the chances of IoT maintaining data privacy but exposing its weaknesses. Most people influence the issues of IoT in data privacy as they are not attentive to the privacy policies of a device or anything they download from the Internet. It reduces the increased corporate transparency as their products and services can be accessed by unauthorized persons (Loukil et al., 2017). The users are expected to maintain data privacy by ensuring IoT increases the organization's transparency which they need to ensure their privacy is maintained and no other people can access personal data (Kamin, 2017). The transparency is not dependent on the Internet of things alone, but it focuses on the governmental regulation or industry self-regulation that needs the organization to get meaningful and informed consent from the clients before they collect any data.

IOT SECURITY AND PRIVACY ISSUES

SECURITY ISSUES

It starts with public perception. The Internet of Things does not take off the needs as the essential things that manufacturers should address. Consumers always question the connected devices, and they are not willing to purchase them since they cannot trust IoT to maintain their privacy (Zhou et al., 2017). There is also vulnerability to hacking whereby the hackers have had to access market devices with energy and enough time. They can also replicate IoT devices where they can hack and access the user's privacy. The companies are ready to deploy the Internet of things devices, but they are not confident if they will secure it from hackers, which proves that the data privacy issue is not well handled as per the reviews (Dai et al., 2017). Finally, identifying is IoT will offer proper security to the devices is a primary concern as securing such devices means that the actual devices themselves are secured more. Thus, to avoid such doubts, the companies should create

security into network connects and software applications that link to the devices, which will prove data privacy.

PRIVACY ISSUES

The amount of data that IoT devices generate is high. Thus, this creates entry points for the hackers who can access the sensitive data belonging to the organization and the clients. When the public knows such information, the chances of engaging in business with such companies are low as they believe the IoT devices in the organization do not consider data privacy (Adams, 2017). There can also be an issue on unwanted public profile whereby the users agree to various terms and condition which are not favorable to what you wish. This type of ignorance directs to the reduction in data privacy as unauthorized individuals can access any information without the client's consent. For example, an insurance company can track and collect information about how a person drives a vehicle when such cars are connected. The device's connectivity can make the hackers and manufacturers invade into a person's privacy, leading to a process called eavesdropping (Vadrevu et al., 2017). Finally, when such things occur as IoT cannot maintain data privacy, consumer confidence in purchasing connected products reduces as they always feel insecure and attacked by making IoT unable to fulfill its potential.

HOW THE RESEARCH WILL HELP THE UNITED STATES

The study of the Internet o Things and Data Privacy is advantageous to the organizations and citizens in the United States who will be aware of what surrounds IoT and what they should do to benefit from it. The relationship between IoT and data privacy helps the users know how knowing more about the terms and conditions may lead to trust issues between the consumers and the organization. The clients are always blaming the company for using the IoT devices when hackers access the information, which makes them avoid operating or purchasing anything from such companies (Lee et al., 2017). Through this, the organizations in the United States should ensure the consumers are aware of what can happen when they decide to use IoT devices. Therefore, to maintain data privacy, the discussion approves increased corporate transparency to solve the problem. Transparency ensures that the organization discloses all the information to the consumer, including if the IoT devices are connected. The clients are aware of how they can prevent hackers from accessing essential information from their devices. The study is also necessary to the United States as people and organizations will determine the connection between IoT and data privacy. In current cybersecurity situations, all devices are bound to hacking, and most people are always unaware of how the cases occur (Ren et al., 2017). With this regard, the discussion above has provided information on how the IoT and data privacy issues are achieved. Hence, such ideas can help individuals protect their devices and ensure hackers do not easily access them as this allows the Internet of things to continue developing.

Splitting the privacy issues and security issues is necessary to the organizations and citizens in the United States. From the privacy issues, they can learn that in IoT, various software and hardware interconnect devices increase the chances of sensitive data leaking through unauthorized individuals. Secondly, without encryption, the devices can transmit user's information. From security risks, they learn that IoT devices are connected to the laptop and desktop, and if there is a lack of security, the personal data will be leaked (Pagallo et al., 2017). Besides, unauthorized manipulation might exploit the security vulnerabilities that can build risks to users' physical safety. The vulnerabilities of IoT devices make the user's network to be harmful and attack other systems. With this information, the organizations and citizens will know what IoT and data privacy can do to the country.

CONCLUSION

In conclusion, IoT can be classified as an essential technology development that assists in discovering issues related to data privacy, which is essential to the people and enterprises in the United States. IoT is the emerging realm of technology that has drawn the attention of researchers around the world. Researchers have also proved that the Internet of Things is under development as many vital concerns connected to privacy and security do not have advanced Research. In this paper, it’s clear the IoT is linked with threats to user's

information as the devices are easily accessed by unauthorized. IoT devices generate high data; therefore, if the system is hacked, it acts as a big blow to the user who nowadays prefers not to purchase IoT products connected. There is also a lack of compliance that brings about data privacy issues under the Internet of things. When the users are not keen on privacy policies, it is more likely for their devices to be tracked as they are not aware and may lose essential information. The primary privacy and security issues surrounding IoT include device heterogeneity, identification, and authentication. The problems relate to how data is vulnerable to breaches and surveillance. The enterprises can avoid this by making their privacy and security protection better. Besides, being transparent also helps the organization allow people to learn how IoT connects with issues in data privacy as it will help them know why and how they can protect their devices. In the end, countries like the United States can apply such studies in creating awareness about IoT and concerns on data privacy. It will help the citizens and enterprises in development.

REFERENCES

1) Adams, M. (2017). Big data and individual privacy in the age of the internet of things. Technology Innovation Management Review, 7(4).
2) Ali, M. S., Dolui, K., & Antonelli, F. (2017, October). IoT data privacy via blockchains and IPFS. In Proceedings of the seventh international conference on the internet of things (pp. 1-7).
3) Banafa, A. (2017). Three major challenges facing iot. IEEE Internet of things.
4) Chernyshev, M., Baig, Z., Bello, O., & Zeadally, S. (2017). Internet of things (iot): Research, simulators, and testbeds. IEEE Internet of Things Journal, 5(3), 1637-1647.
5) Dai, W., Qiu, M., Qiu, L., Chen, L., & Wu, A. (2017). Who moved my data? Privacy protection in smartphones. IEEE Communications Magazine, 55(1), 20-25.
6) Daud, M., Khan, Q., & Saleem, Y. (2017, November). A study of key technologies for IoT and associated security challenges. In 2017 International Symposium on Wireless Systems and Networks (ISWSN) (pp. 1-6). IEEE.
7) Frustaci, M., Pace, P., & Aloi, G. (2017, September). Securing the IoT world: Issues and perspectives. In 2017 IEEE Conference on Standards for Communications and Networking (CSCN) (pp. 246-251). IEEE.
8) Javed, B., Iqbal, M. W., & Abbas, H. (2017, May). Internet of things (IoT) design considerations for developers and manufacturers. In 2017 IEEE International Conference on Communications Workshops (ICC Workshops) (pp. 834-839). IEEE.
9) Kamin, D. A. (2017). Exploring security, privacy, and reliability strategies to enable the adoption of IoT.
10) Lee, S. K., Bae, M., & Kim, H. (2017). Future of IoT networks: A survey. Applied Sciences, 7(10), 1072.
11) Loukil, F., Ghedira-Guegan, C., Benharkat, A. N., Boukadi, K., & Maamar, Z. (2017, October). Privacy-aware in the IoT applications: a systematic literature review. In OTM Confederated International Conferences" On the Move to Meaningful Internet Systems" (pp. 552-569). Springer, Cham.
12) Pagallo, U., Durante, M., & Monteleone, S. (2017). What is new with the internet of things in privacy and data protection? Four legal challenges on sharing and control in IoT. In Data protection and privacy :(In) visibilities and infrastructures (pp. 59-78). Springer, Cham.
13) Punia, A., Gupta, D., & Jaiswal, S. (2017, May). A perspective on available security techniques in IoT. In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (pp. 1553-1559). IEEE.
14) Ren, Z., Liu, X., Ye, R., & Zhang, T. (2017, July). Security and privacy on internet of things. In 2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC) (pp. 140-144). IEEE.
15) Terry, N. (2017). Existential challenges for healthcare data protection in the United States. Ethics, Medicine and Public Health, 3(1), 19-27.
16) Vadrevu, P. K., Adusumalli, S. K., & Mangalampalli, V. K. (2017). Survey: Privacy Preserving Data Publication in the age of Big Data in IoT Era.
17) Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. V. (2017). Security and privacy for cloud-based IoT: Challenges. IEEE Communications Magazine, 55(1), 26-33.