Impact of Internet of Things on Data Privacy

Masum Patel

Department of Computer Science, Monroe College, King Graduate School

KG604: Graduate Research & Critical Analysis

Professor Jonathan Kyei

2/28/2023

Impact of Internet of Things on Data Privacy

Introduction to Literature Review

The Internet of Things (IoT) may have a substantial influence on people's privacy as more data from many sources is gathered utilizing these devices, with the extra possibility of comprehensive monitoring of people without their knowledge or agreement (Caron et al., 2016). This literature review will help to promote a safe and trustworthy sharing of personal information, avoid unintended and unethical use of gathered IoT data, and address the rising concern about individual privacy in the IoT space. Only those publications that discuss the Internet of Things and its security issues with regard to preserving personal data privacy are taken into the account in this literature assessment. The factors that were included in this literature review were the challenges, risks, and concerns of the existing measures of protecting individual privacy, the limitations of privacy measures of people's data collected in the IoT, and the measures that can be put in place to protect individual privacy. This literature search process was possible through the Monroe College Library databases, including ProQuest and EBSCO Host. The main terms that were used to select the most relevant articles are individual privacy, internet of things (IoT), privacy legislation, intelligent homes, and privacy issues.

Review of Literature

Impacts of IoT on Individual Privacy

Caron et al. (2016) set out to conduct a study on the concept of the internet of things (IoT) and the impact of this concept on the privacy of individual data. The three researchers, Xavier Caron, Rachelle Bosua, Atif Ahmad, and Sean B. Maynard, collected data in 2015 in Australia with the purpose of determining the effect that the IoT has on the privacy of individual information. The authors of this article used a systematic literature review of to find relevant data

for the study topic. The two-step systematic research started with phase 1, which was the process of searching for, identifying, and selecting the most relevant literature. The additional phase was a content analysis of the literature to help identify themes that show the critical concerns of the individual users. The purpose of the study was to determine if the Australian Privacy Principles (APP) are sufficient to safeguard Australian citizens' privacy, particularly those who use the Internet of Things. According to the study's conclusions, IoT data gathering and individual privacy are both constrained by the present APP. The research revealed that the data protection measures were insufficient. These restrictions have an effect on how personal data is gathered, utilized, and handled.

Apart from Australia, other research on the same issue was based in other nations. Aleisa and Renaud (2016) used a systematic literature review to collect data in 2016 in three focus countries including France, Germany, and Italy. Noura Aleisa and Karen Renaud, conducted this research with the goal of exploring the aspects of privacy of IoT on individual data, and how the main areas that require attention. Aleisa and Renaud (2016) conducted a thorough quantitative literature study to evaluate the privacy boundaries that the IoT may possibly breach. Comparing the approach to the narrative research style, it offers advantages. Aleisa and Renaud (2016) used a systematic literature review that is ideal in identifying the gap in knowledge in the internet of things research. The researchers demonstrated that there is growing awareness about the various dangers to information and identified potential countermeasures. One of the key issues is the growing gathering of personal data, particularly the dangers that come from data mining techniques used to analyze personal data.

According Aleisa and Renaud (2016), sharing of unanonymized data (25.9%) and location tracking, approximately 31.5% of the studies, are the two biggest areas of concern.

Inventory assaults (8.3%), interaction and presentation (6.5%), life cycle transitions (3.7%), and linking (2.7%) were the next most common topics of concern in the articles, with 21.3% of the publications mentioning profiling-related issues. Several suggested solutions need close interaction between humans and the process. Several solutions use privacy-aware software or access control techniques. The research suggested the Dynamic Privacy Analyzer (DPA), a tool to inform owners of smart meters' data about the privacy dangers associated with doing so. On the other hand, approximately half of the suggestions called for eliminating the human from the process. To prevent data from being snooped on the way to servers, they suggested employing cryptographic methods and information modification, or data reduction.

Smart Home Systems and Individual Data Privacy

Marafa et al. (2021) reviewed the impact of IoT on the privacy of individuals in smart home systems. The authors collected data in 2018 in Nigeria using a systematic review. The goal of the study was to determine how smart home systems impact the privacy of individuals from the Nigerian perspective. The authors explained how they acquired the papers for the study based on the systematic review of data gathering. The authors then went on to more depth about pertinent topics such as search terms, article sources, research selection, eligibility requirements, and data collecting procedure. According to the research, intelligent home systems come with many difficulties. The difficulties may lie in the system's inherent weaknesses, where the structure's construction makes it vulnerable to several attacks. Examples of such assaults include those made against firmware, hardware, system applications, data, and network interfaces or ports. The system may also be vulnerable to network-related attacks and protocol failure because of bidirectional communication relationships between objects. Information leaks, insufficient data, and illegal attacks are possible additional pertinent threats.

Zeng et al. (2017) did a comparable study which aimed to identify end user security in the United States. Zeng et al. (2017) conducted interviews in the US in the year 2017 concerning the end-user security and privacy concerns of smart homes. The goal of the study was to investigate the concerns associated with the privacy and security of smart homes. The researchers performed an exploratory interview with a colleague who installed and resided in an intelligent house before creating the interview questions. They performed four more pilot interviews with occupants of smart homes after creating the original interview questions, and they revised the questions to clarify the comments and more effectively address the study's research topics. The results demonstrated that different people had different worries and defense mechanisms in response to security and privacy issues. Participants lack a shared set of worries or mitigations and have different and sparse threat models.

Analysis of Literature

When more data from many sources is acquired via these devices, along with the additional prospect of extensive surveillance of individuals without their knowledge or consent, the Internet of Things (IoT) may significantly impact people's privacy. Researchers have investigated IoT's impact on individuals' privacy (Caron et al., 2016; Aleisa and Renaud, 2016). While Caron et al. (2016), Aleisa and Renaud (2016), and Marafa et al. (2021) used a systematic literature review, Zeng et al. (2017) chose an interview method. Also, the first two sets of researchers investigated the impact of IoT systems, while the last two went further to investigate the impact of smart home systems for more clarity. Caron et al. (2016) purposed to determine if the Australian Privacy Principles (APP) are sufficient to safeguard Australian citizens' privacy, particularly those who use the Internet of Things. According to the study's conclusions, IoT data gathering and individual privacy are both constrained by the present APP. According to Marafa

et al. (2021), smart home systems come with a lot of difficulties. The difficulties may lie in the system's inherent weaknesses, where the structure's construction makes it vulnerable to several attacks. Similarly, Zeng et al. (2017) demonstrated that different people had different worries and defense mechanisms in response to security and privacy issues. Aleisa and Renaud (2016) suggested employing cryptographic methods and information modification, or data reduction to prevent data from being snooped on the way to servers.

References

Caron, X., Bosua, R., Maynard, S. B., & Ahmad, A. (2016). The Internet of things (IoT) and its impact on individual privacy: An Australian perspective. *Computer Law & Security Review*, *32*(1), 4-15. https://doi.org/10.1016/j.clsr.2015.12.001

Aleisa, N., & Renaud, K. (2016). Privacy of the Internet of Things: A Systematic Literature Review (Extended Discussion). *ArXiv (Cornell University)*. https://arxiv.org/pdf/1611.03340

Marafa, F. M., Sa'ad, S., Tukur, A., & Mohammed, A. (2021, April). A Review on Impact of Internet of Things (IoT) on Individual Privacy in Smart Home Systems. In 2021 *2nd International Conference on Intelligent Engineering and Management* (ICIEM) (pp. 127-131). IEEE. doi: 10.1109/ICIEM51511.2021.9445330.

Zeng, E., Mare, S., & Roesner, F. (2017, July). End user security and privacy concerns with smart homes. In *Symposium on Usable Privacy and Security (SOUPS)* (Vol. 220). https://www.usenix.org/system/files/conference/soups2017/soups2017-zeng.pdf