

Differential Privacy Strategies for Improving Privacy on the Internet of Things

¹ Sharmila S, ² Kanagaraj A, ³ Finny Belwin A, ⁴ Linda Sherin A, ⁵ Dr. Antony Selvadoss

Thanamani

^{1,2,5} Department of Computer Science, Nallamuthu Gounder Mahalingam College, Pollachi,
Coimbatore, TamilNadu, India

Email - ¹ mcasharmi2007@gmail.com, ² a.kanagaraj@gmail.com, ⁵ selvdoss@gmail.com

³ Department of Computer Science, Angappa College of Arts and Science, Coimbatore,
TamilNadu, Email - belwin35@gmail.com

⁴ Department of Computer Science, AMJAIN College, Chennai, TamilNadu, Email -
linz15sherin@gmail.com

Abstract

The Internet is receiving and storing an enormous amount of data thanks to recent advancements in communication and data storage technologies. Organizations do not want to share their information for legal or competitive reasons, despite the fact that such a vast volume of data gives significant opportunity for knowledge development. This brings up the issue of data mining while maintaining privacy. Current data mining privacy preservation strategies are based on the assumption that all intermediate outcomes from data mining processes are suitable for publication. However, it has been demonstrated that such intermediate outputs might nonetheless leak private data. In this case, differential privacy is applied to quantitatively limit information leakage. Differential privacy is a new idea in privacy that can provide strong, observable privacy assurances. The extensive deployment of low-cost smart gadgets and the ubiquitous use of high-speed wireless networks has been aided by the rapid expansion of the Internet of Things (IoT). IoT welcomes a variety of physical artifacts that have not before been active on the Internet, allowing for a wide range of IoT applications to be given through their interaction and cooperation. Many IoT services necessitate a thorough understanding and analysis of data acquired from a large number of physical devices, posing a threat to both personal data privacy and IoT creation. IoT data privacy is a broad and complicated phrase, as people's perceptions and interpretations differ, and it necessitates legislative and technological measures to implement. In this paper we review IoT privacy enhancement using different privacy strategies on various IoT applications and challenges with Security & Privacy.

Keywords: Internet of Things, Differential Privacy, Security, Privacy, Data Mining, Data Set, Server.