CS543 - Paper Review Report # IV

Hailu Belay Kahsay - 20155624

Title: Big Data Privacy in the Internet of Things(IoTs) Era

Author: Charith Perera, Rajiv Ranjan, Lizhe Wang, Samee U. Khan, Albert Y. Zomaya

The paper starts by defining IoT, is a network of networks in which a massive number of objects, sensors, or devices are connected through the ICT infrastructure to provide value-added services, and big data, has no clear definition. In the paper it is shown that big data is not wholly about size rather it is defined with three primary characteristics, also known as the 3Vs: volume(relates to the data's size), variety(the type of data and its source), and velocity(how frequently the data is generated). Since the data collected by smart IoT devices may contain sensitive personal information based on the application type and the data source, they must be managed carefully to avoid any user privacy violations.

In the paper it is shown that privacy concerns could be a significant barrier to the IoT's growth due to the fact that the IoT is more vulnerable to privacy violations than the web era. Unlike today's network in the future IoT era it's likely that service providers will adopt one of the following models to gather information: some consumers might willingly pay to consume services with the aim of protecting their privacy; others might offer to give away data, under some limitations and conditions, in return for consuming services free of charge. As per the EU commission report security and privacy has been identified as a major IoT research challenge that encompasses privacy-preserving technology for heterogeneous device sets; models for decentralized authentication and trust; energy-efficient encryption; data-protection technologies; security and trust for cloud computing; data ownership; legal and liability issues; repository data management; access and use rights; rules to share added value; responsibilities; liabilities; artificial immune system solutions for the IoT; secure, low-cost devices; integration with or connection to privacy-preserving frameworks; and privacy policies management.

In the paper some of the major IoT privacy challenges, such as , User consent acquisition, Control, customization, and freedom of choice, Promise and reality, Anonymity technology, and Security has been introduced and discussed. In order the current IoT solutions gain customers' confidence the technology should support a privacy-guaranteed data management lifecycle. That is from the time the data is captured by the sensors embedded in IoT solutions to the point at which knowledge is extracted and raw data is permanently and securely deleted, user privacy must be protected and enforced. In order to do so, five major stakeholders that are responsible for protecting user privacy: Device manufactures, IoT cloud services and platform manufacturers, Third-party application developers, Government and regulatory bodies, and Individual consumers and non-consumers, have been identified.

Finally, the paper talks about the state of the art: the EU-funded OpenIoT project, Microsoft Research's Lab of Things (LoT), The Hub of All Things, Xively that offers a platform as a service, Datacoup that let users sell personal data, Mydex that helps individuals to hold, control, and reuse their personal information in effective and secure ways, and Mydex, a personal data sharing platform.