Data Ethics in IoT

Gehad AlaaElDin 3743[Computer & Communications]

Aliaa Abbas 3747[Computer & Communications]

Mohamed Khamis 3823[Computer & Communications]

Mayar Mohamed 3856[Computer & Communications]

Shahenda Zakaria 3890[Computer & Communications]

Merna Zakaria 4106[Computer & Communications]

Instructors:

Dr. Mohamed Hassan, Dr.Mohamed Ghazy

Abstract:

The purpose of this study is to treat aspects that are related to the sensitivity of data, information and knowledge transmitted through Internet of Things, helping all people interested in these new ICT technologies to become aware of some ethical issues. In this new media, which is no more in its infancy, the vulnerabilities and attacks are various, caused by technological advances and proliferated through lack of users' awareness. This warning message is needed because of data, information and knowledge transfer from virtual to physical devices that are connected to wireless networks of different sizes and importance. The transfer is augmented by the extended use of new technologies as RFID, NFC, sensors, 3G and 4G and brings along the adjustment of the traditional information security threats to this new environment, as well as the emergence of new characteristic dangers. The problems treated here are of interest both for each of us, as individuals, and for the organizations managers – especially in a world in which the borderline between the physical and virtual life is becoming more and more difficult to draw.

1. Introduction:

1.1 Motivation:

The technological developments and the evolution of the modern world to include the virtual as well as the physical world in what is called the Internet of Things has significantly improved standards of living.

Data gathered through the IoT has incredible potential for improving user experience and building a better city. **[1]**

The IoT creates endless streams of data, and the possibilities for harnessing that data are endless. However, it does not come without its problems. In fact, there are three major challenges concerning the IoT that we cannot ignore:

- Ubiquitous data collection.
- Potential for unexpected uses of consumer data.
- Heightened security risks.

These issues raise a number of ethical and legal questions around the IoT and the data it collects and processes, as it raises risks to the privacy, security and potential exploitation of users.

1.2 Background:

The **Internet of things** (**IoT**) is the network of physical devices, vehicles, home appliances, and other
items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to connect and exchange data.**[2]**

The IoT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct

integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in

addition to reduced human intervention. When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber physical systems, which also encompasses technologies such as smart grids, virtual power plants, smart homes, intelligent transportation and smart cities.**[3]**

These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices.**[4]**

The Internet of Things provides fertile ground for marketing, but it is a minefield for the Ethical Use of Data (EUoD). As consumers adopt a more connected lifestyle, the responsibility of how this information is collected, shared and applied will become increasingly complex, and essentially impossible for the consumers themselves to be fully accountable for.

Most consumers are not preoccupied with knowing exactly how data about themselves is collected, analyzed and used. Consider how often the average person actually reads privacy policies before agreeing to the terms – not often. Instead, consumers pick brands they trust, and expect them to take proper precautions to keep the data safe and use it responsibly.

This is a shift of the accountability burden from the consumer to brands. Brands that want to operate with confidence and demonstrate their trustworthiness to their customers should begin the process of being accountable for the EUoD. This requires a few things: A commitment to respecting consumer privacy and policies that reflect accountability for ethical use; mechanisms to put policies into effect; monitoring to assure mechanisms work; providing consumers transparency and choice

opportunities; and standing ready to demonstrate and remediate when necessary. In other words, the operationalization of data use ethics.**[5][6]**

One of the key drivers of the IoT is data. The success of the idea of connecting devices to make them more efficient is dependent upon access to and storage & processing of data. For this purpose, companies working on IoT collect data from multiple sources and store it in their cloud

network for further processing. This leaves the door wide open for privacy and security dangers and single point vulnerability of multiple systems. The other issues pertain to consumer choice and ownership of data and how it is used.

A report published by the Federal Trade Commission (FTC) in January 2015 made the following three recommendations:**[7]**

- **Data security** – At the time of designing IoT companies should ensure that data collection, storage and processing would be secure at all times. Companies should adopt a "defence in depth" approach and encrypt data at each stage
- **Data consent** – users should have a choice as to what data they share with IoT companies and the users must be informed if their data gets exposed.
- **Data minimization** – IoT companies should collect only the data they need and retain the collected information only for a limited time.

1.3 Objectives:

The aim of the paper is to raise awareness around the underlying system of the IoT and the potential risks and problems that may arise as a result of it as well as suggest possible actions taken to tackle and limit the onset of these issues.

2. Risks of IoT devices:

As expected of a new era of technology that involves “smart” devices monitoring aspects of people’s everyday life, saving this data on cloud servers and running them through AI algorithms to get predictions and analysis of people’s behaviors. The risks involve but are not exclusive to the following:

2.1 Data Security
2.2 Information Privacy & Protecting consumers from spying.
2.3 Exploitation of users.

We shall discuss Three cases in which the three subjects were compromised, the outcome of such cases on parties involved and how managers attempted to limit the effect of them.

2.1 Data Security:

As IoT thrives on collecting big data from sensors and actuators, this data is subsequently saved on cloud servers. This poses security risks on clients data which are exposed to hackers if the organization were not careful in properly securing them. Regardless of whether or not the data were of sensitive nature or if users may or may not have objections to it being exposed it is not good practice to leave such information unsecured.

Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings

A company that sells internet-connected teddy bears that allow kids and their far-away parents to exchange heartfelt ***messages left more than 800,000 customer credentials, as well as two million message recordings, totally exposed online for anyone to see and listen.***

Since Christmas day of last year and at least until the first week of January, Spiral Toys left customer data of its CloudPets brand on a database that wasn't behind a firewall or password-protected.
The MongoDB was easy to find using Shodan, a search engine makes it easy to find unprotected websites and servers, according to several security researchers who found and inspected the data.

The exposed data included more than 800,000 emails and passwords, which are secured with the strong, and thus supposedly harder to crack, hashing function “bcrypt”. Unfortunately, however, a large number of these passwords were so weak that it's possible to crack them, according to Troy Hunt, a security researcher who maintains Have I Been Pwned and has analyzed the CloudPets data.

During the time the data was exposed, at least two security researchers, and likely malicious hackers, got their hands on it. In fact, at the beginning of January, during the time several cybercriminals were actively scanning the internet for exposed MongoDB's databases to delete their data and hold it for ransom, CloudPets' data was overwritten twice, according to researchers.

Two researchers warned Motherboard of this security breach independently in the last few weeks. With their help, Motherboard was able to verify that the breach was legitimate.

The CloudPets database is making the rounds in the internet underground, according to both Hunt and Victor Gevers, the chairman of the non-profit GDI Foundation which discloses security issues to affected victims. Gevers saw the database while it was exposed online at the end of last year, and said ***it contained data on 821,396 registered users, 371,970 friend records (profile and email) and 2,182,337 voice messages.***

The voice messages themselves were not in the database, according to the researchers. But Hunt found out that they were stored in an Amazon S3 bucket that doesn't require authentication. So as long as hackers could guess the URL of the files, they could listen to the messages. Hunt said he believes that was definitely possible. Moreover, many customers used

incredibly weak passwords such as 123456 or "cloudpets" making it trivial to log into their accounts and listen to the saved messages.

Article References: [8][9][10]

Comments:

The incident above highlights the vulnerability of data acquired from IoT devices to hacking. All it takes is an irresponsible organization not properly securing the data it collects and the users' information were available to unauthenticated parties.

However, securing users data is far from an impossible task and companies can manage to secure their cloud servers and client information.

Ethical Implications:

Ethical issues and risks arise when companies are not bothered to provide their users with proper security, it is hard to monitor and regulate this as virtually anyone can produce IoT devices to the public, sometimes individuals or small organizations that may not be very efficient in securing their databases.

2.2 Information privacy:

Agreeing upon what kind of data agencies are allowed to collect and use and what cannot is a major concern, information such as location and destinations and daily activities captured through social media as well as from IoT devices like phones can be used to spy on individuals and frisking them to know their habbits.

Samsung smart TVs send unencrypted voice recognition data across internet

Samsung smart TVs are sending users' voice searches and data over the internet unencrypted, allowing hackers and snoopers to listen in on their activity.

The revelation comes 10 days after Samsung found itself in the middle of a row over the "Orwellian" privacy policy" for its smart TVs, after it was revealed that it was sending user voice data to third parties.

It was believed that the information was encrypted but now a security expert has found that data is vulnerable while in transit. Samsung had stated that it uses "industry-standard security safeguards and practices, including data encryption, to secure consumers' personal information and prevent unauthorised collection or use", in a blog post clarifying its privacy policy.

When a user carries out a voice search using a smart TV the audio is sent across the internet to a voice recognition service that interprets the speech and sends back the results in text.

In some Samsung models, neither the audio, nor the text returned, is being encrypted, meaning hackers or snoopers can clearly see the words and phrases that users speak to the TV. The television also sends other personal information about the TV and user in the unencrypted information.

The smart TVs, which can be operated by voice commands to adjust channels, can be used with natural language search. They can be activated with hot word "Hi TV", which the television can be set to always listen out for. Samsung uses voice recognition company Nuance to power its voice command services.

Article References: [11][12] [13]

Comments:

The second downside regarding IoT is recurrent with major companies reportedly being involved in gathering data **involuntarily** from customers, Samsung only warned its users through small print on their privacy license that they were being listened to all the time and their

conversations were being sent to third parties across the internet, the mega company only advised customers ***not to talk of sensitive or private issues while using their voice recognition system*.**

Ethical Implications:

The incident with Samsung openly admitting it were virtually spying on its customers is not a first of its kind, but every software or company implementing voice recognition systems is guilty of the same, privacy concerns have expanded to beyond voice records or insecure webcams or GPS tracking devices into all devices in their homes, with even government officials professing to potentially using data from smart homes and such to monitor human behaviors

2.3 Exploitation of users:

Guaranteeing private sectors won't exploit the behavior patterns they can detect through data. With the increase in cameras, voice recorders, GPS and different sensors and monitors constantly recording users' statuses, it is a modern dilemma how companies are allowed to use such information and who gets to access them. recent software developments in machine learning and predictive analysis puts clients at risk of their behaviors being monitored by agencies and exploited for profit.

Facebook Launches New Privacy Policies and You Still Can Be Used For Ads

Facebook confirmed it's able to ***use the postings and personal information of 1.2 billion accounts on the service for advertising purposes***. The social media website announced the new privacy policies in a blog post on the site.

Facebook initially included, then removed, a line about how minors who join the site needed a parent or guardian to give consent before they are used in ads. Facebook now says that this permission is granted once the teen signs up for the site.

The changes were first proposed by Facebook in August 2013, then drew the attention of the Federal Trade Commission after privacy groups complained in September that Facebook was exploiting minors.

The changes followed Facebook's $20 million settlement in August of a class action lawsuit that claimed the company's "Sponsored Stories" platform had shared users' "likes" without paying them or allowing them to opt out**.**

In 2011, Facebook and the FTC had reached a separate settlement over alleged privacy violations by the site. Facebook agreed to scheduled checkups by "independent, third-party auditors" over the next 20 years to ensure that the company's privacy policies and practices do not violate users' rights.

In the blog post Friday explaining the policy, Facebook Chief Privacy Officer Erin Egan said the sentence regarding minors did not grant the company any additional rights over user content. After receiving feedback, the company agreed "that the language was confusing" and "removed the sentence."

Despite Facebook's clarification, many members of the site remain confused about their privacy options. In the August settlement, Facebook was ordered to implement provisions to make its user privacy policy more transparent. One part of the policy says the company will give parents the chance to prevent their children's information from being used in ads, and that the site will let users know if any comments they made on the site were turned into a "Sponsored Stories" ad, giving them the chance to opt out.

"The innovative controls we agreed to in connection with the settlement take time to build," Jodi Seth, a Facebook spokeswoman told The New York Times in a Friday story. She offered no timetable for introducing them.

Article References: [14][15] [16]

Comments:

The recent developments in machine learning with the CEOs of “free” internet sites looking for profit has led to the increase in recommender systems and online advertisements, this is at the expense of users’ privacy and information, it has been inferred that social media websites are only free because the webpages are not the merchandise they’re selling, but rather the users themselves, a great percentage of income of such companies is of ads (constituting as much as **90%** of Google’s income**)** Companies manage this by surveying users posts and ad clicks and even browser history for their preferences and directing clusters of ads serving their purposes at them at them

Ethical Implications:

Future solutions to ethical concerns of advertising online should not only look at truthfulness of advertisements, but also the transparency for how information gathered from users is stored and sold. The ethics of building a business off of selling the massive amounts of information with no choice to opt-out is also a current issue within the online advertising market. Most consumers know and accept that various "bonus" cards at retail stores enable companies to gather information, but the rewards or bonuses they offer make the deal acceptable. The current online trend is a difficult opt-out program that involves constantly finding new ways to block online entities from tracking users

2.4 Recommendations:

2.4.1 Develop IoT Standards

Having a universal standard for IoT designers allow designers and developers, whether in entities or individuals to employ user-friendly and secure products, it would allow marketers to focus on user experience and be able to fulfill potential for innovation and efficiency. These standards must cover everything from technical to legal and ethical issues of IoT.

2.4.2 Simplified Terms of Use and opt-out Options

It seems that “Notices and Guidelines” of possible breaches of privacy in current “Terms of Use” are rather lengthy fingerprints to force readers to accept them without having much of a say. Due to sensitivity and richness of IoT datasets, such practices cannot continue. Terms of Use of IoT devices must clarify any collection, usage or sharing of data unrelated to the expected function of the device itself. It must also provide an opt-out option.

2.4.3 De-Identification is Not Enough

A critical Issue is that companies are allowed to gather involuntary data without consent as long as such data is de-identified. However, since technologies exist that identify individuals from unidentified and unassociated datasets, it is required to establish laws such that risk of identification is spelled out

2.4.4 Complete Transparency even after consent

Even after users agree to Terms of Use, companies must be fully transparent on what data they collect, who gets access to it, what purposes it deploys them to and most importantly how they keep data secure, an option to revoke consent later with knowledge of previously acquired datasets is also important.

2.4.5 Establish laws to limit nonconsensual use of IoT data

Industries such as insurance are eager to use IoT. Insurance is as important as credit, employment and housing, usage of IoT for insurance decisions must be regulated and also require explicit “Notice and Choice”

3. Conclusion:

The Ethical and legal uncertainties relating to deploying the IoT are spurious and are not yet directly addressed due to the field being yet in its early stages of development, it's observed that the problems which have arised so far have not been properly addressed or solved, as both companies and individuals have dismissed the complications of the issues. It is therefore the responsibility of governing bodies to set rules and regulations limiting how far companies can set to collect data and how freely they can deploy it into analysis and decision making. This does not exempt organizations from having the ethical & moral obligations to not take their customers information for granted and not use it for profit without their consent.

References:

1 http://data.london.gov.uk/blog/the-trouble-with-the-internet-of-things/

2 http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

3 http://www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf

4 http://data.london.gov.uk/blog/the-trouble-with-the-internet-of-things/

5 https://www.forbes.com/sites/ciocentral/2016/12/21/on-the-ethical-use-of-data-vs-the-internet-of-things/#2b3b47111247

6 http://www.canadiancybersecuritylaw.com/2015/11/the-internet-of-things-guidance-regulation-and-the-canadian-approach/

7 http://fortune.com/2016/04/06/who-owns-the-data/

8 https://iapp.org/news/a/breach-of-smart-teddy-bear-data-leaks-800000-users-info/

9 https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/

10 https://motherboard.vice.com/en_us/article/pgwean/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings

11 https://www.cnet.com/news/samsungs-warning-our-smart-tvs-record-your-living-room-chatter/

12 https://www.cbsnews.com/videos/samsung-smart-tvs-voice-recognition-creates-privacy-concerns/

13 https://www.theguardian.com/technology/2015/feb/19/samsung-smart-tvs-send-unencrypted-voice-recognition-data-across-internet

14 https://www.techrepublic.com/article/facebook-exploited-emotions-of-young-users-to-sell-ads-leaked-document-says/

15 https://www.utc.edu/center-information-security-assurance/pdfs/ethical-issues-of-online-advertising-and-privacy.pdf

16 https://www.huffingtonpost.com/2013/11/16/facebook-privacy-policy_n_4288916.html