Title
THE FUTURE OF PRIVACY AND CYBERSECURITY

Journal
Berkeley Scientific Journal, 22(2)

ISSN
1097-0967

Author
ZENG, JENNIFER

Publication Date
2018

DOI
10.5070/BS3222039580

Undergraduate

THE FUTURE OF PRIVACY AND CYBERSECURITY

BY JENNIFER ZENG

"Big Brother is watching you." But rather than being watched through forced surveillance as George Orwell's *1984* suggests, today, consumers are slowly conceding their own privacy. Already, smart technologies such as refrigerators and thermostats are used without a second thought. With our current rate of technological progress, it is not unreasonable to imagine a future where nearly every tool we use everyday will be connected to the internet. Although the network that connects all these devices—the Internet of Things (IoT)—is only in its early stages, its increasing prevalence will be one of the main issues of next-generation cybersecurity.

Apart from the direct collection and distribution of information, future privacy concerns will revolve around the ability of companies to obtain new information about consumers that is not given voluntarily.[7] Information will be generated through predictive analytics, which is the use of statistics and data modeling to make predictions based on existing data. Data produced through predictive analytics is considered new information; under current informational privacy networks, it is unclear whether the consumer or the analytics company has the right to this data and its dissemination.[2] This issue gives rise to a new model of privacy that consumers must consider—datafication privacy—beyond the current models of surveillance and data collection privacy.

The negative effects of predictive analytics will only be exacerbated by the information consumers unwittingly provide through the IoT. The IoT consists of all smart devices connected to the internet in a residence, such as refrigerators and speakers. Devices connected through the IoT share consumer behavior patterns and other personal information with each other.[4] This is of particular concern because of the increasing popularity of these devices, which are touted for their efficiency and personalizability. Yet consumers are largely unaware of how easily hackable devices on the IoT are, and often consider the information they carry to be benign.

The IoT lacks security for several reasons. Devices have varying authentication methods due to differing environments; because there is no standard protocol for authentication, each device represents a point of vulnerability that could compromise the entire system. The ability of hacked devices in an IoT network to compromise the rest, regardless of any dissimilarity between devices, generates a unique form of vulnerability for such systems. A hacked refrigerator is a threat to a thermostat on the same network because of the general features IoT devices must share in order to communicate. The weak security systems of these devices, and their relatively small size and low-power needs, make IoT devices particularly susceptible to distributed denial of service (DDoS) attacks. A denial of service attack occurs when a computer is overloaded with useless incoming data, so it cannot

"If IoT devices are connected across a blockchain network, the information they share through the network will be cryptographically proofed and secured."

receive any other information; a distributed DoS occurs when the packets are being sent to a single computer from a large number of sources. The largest attack on the IoT thus far was by malware that utilized unchanged default passwords for routers and similar devices to instigate DDoS.[8]

One possible security solution utilizes blockchain technology. Blockchain is a secure-by-design decentralized model of information storage based on cryptography, which means that it is not controlled by a single computer or operator. This minimizes its chances of being compromised. All the information held by the model is distributed to every computer connected across a shared network, rather than being stored with a third party. Information is stored in "blocks" connected by secure links, and changing even one piece of information at any point in the "chain" involves gaining consent from over 50% of the remaining network.[1] If IoT devices are connected across a blockchain network, the information they share through the network will be cryptographically proofed and secured.

Another aspect of blockchain that can be utilized to enhance security is coded contracts. Coded contracts can be used to determine who has access to device software, including patches and updates, as well as who can request service on the device.[6] These contracts are executed on the blockchain, not by a third party, so they cannot be altered. Unlike a regular contract, in which any of the named parties can break the contract while the rest of the parties follow through, all parties mentioned in a coded contract must fulfill their sides of the agreement or none of the terms of the contract will be executed on the network.

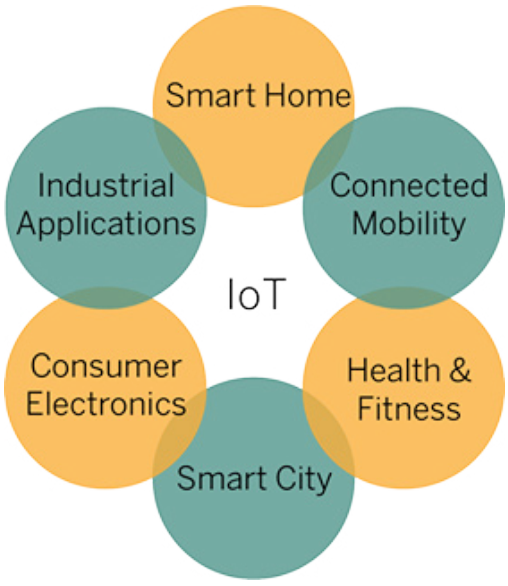

Figure 1. The Internet of Things connects several spheres of electronics.[10]

Artificial intelligence is a second possible solution for security. Deep learning is a subset of machine learning, which in turn is one method of producing AI. Deep learning utilizes information sharing and a computing system that resembles the neural networks in the brain in order to form new connections among information. By analyzing the details of past attacks on a network, deep learning can uncover attack patterns to fix security flaws. Because it is self-learning and requires little supervision, it is more effective and efficient than assigning a person to manually update security protocol every time an attack occurs, especially when the underlying mechanism is too complex for a person to debug. It has been shown that deep learning can be used to detect attacks on IoT networks by utilizing a fog-computing method rather than a cloud-computing method.[5] While cloud computing relies on a central server far away to complete computational processes, fog computing works on the edge of the "cloud" of devices connected to a server, storing data closer to the device in the network that's using it. This increases the efficiency of IoT and allows faster deep learning calculations.

While cutting-edge technology can be used to provide secure-by-design systems, it is still humans who generate these technologies and use them. Thus, the ongoing development of IoT has led to a new facet of security as well: non-technical cyber hygiene on the part of the consumer. Theresa Miedema of the University of Toronto defines cyber hygiene as security measures that consumers should use to protect their privacy and devices through the internet.[4] Because of the increased interaction between consumers and smart devices, bad cyber hygiene can affect not only personal de-

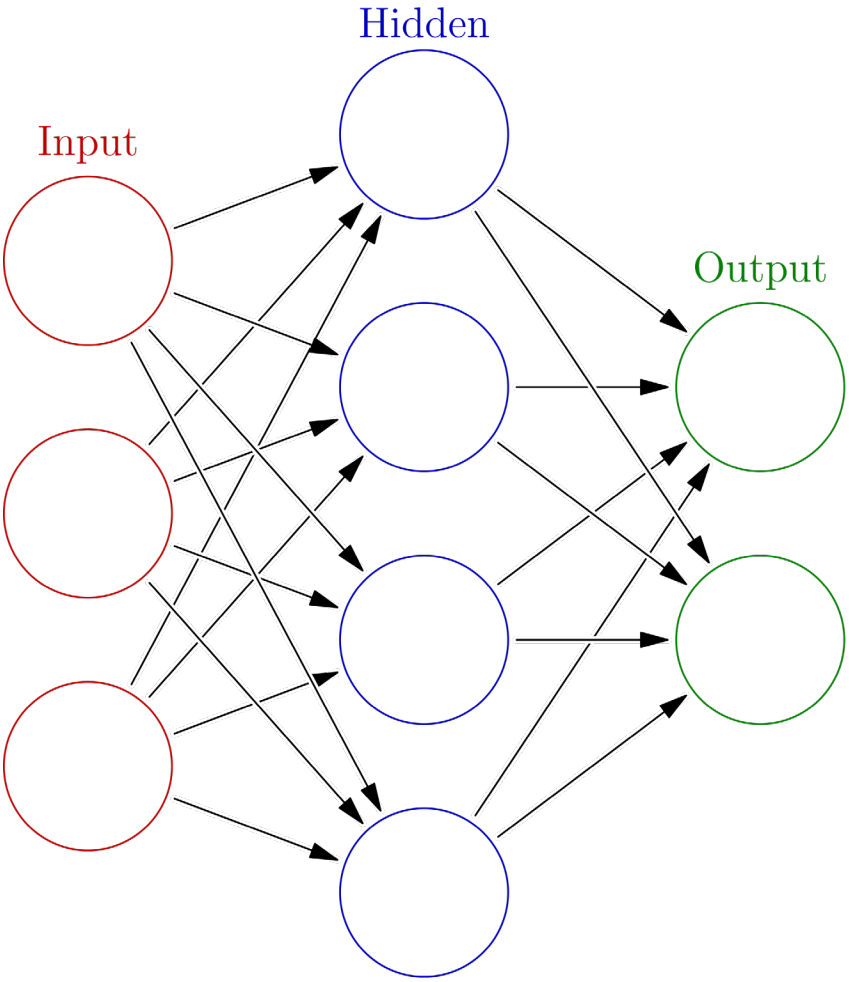

Figure 2. **Artificial neural networks are commonly composed of three layers: input, hidden, and output. The input layer contains passive nodes, which don't modify data, while the hidden and output contain active nodes which do modify data.[9]**

> "By analyzing the details of past attacks on a network, deep learning can uncover attack patterns to fix security flaws."

vices, but also those of everyone else on the same IoT network. Machine learning can be used to recognize patterns in consumer behavior and predict their behavior in order to recognize those that show risky cyber hygiene, such as using manufacture default passwords and forwarding phishing links.[3]

The next generation will deal with security issues that extend beyond what information can be stolen from existing databases. Instead they must grapple with how that information can be used to produce new details about their private lives, as well as the smart devices that will dominate their lives and become a privacy liability. It is critical for consumers, even now, to be aware of potential security vulnerabilities in and data collection by the most basic internet-connected devices around them.

REFERENCES

1. Kshetri, N. (2017). Blockchains roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 41(10), 1027-1038.
2. Mai, J. (2016). Big data privacy: The datafication of personal information. Information Society, 32(3), 192-199.
3. Srinivasan, R. (2017). How Machine Learning Can Help Identify Cyber Vulnerabilities. Harvard Business Review Digital Articles, 1-4.
4. Miedema, T. E. (2018). ENGAGING CONSUMERS IN CYBER SECURITY. Journal Of Internet Law, 21(8), 3-15.
5. Diro, A. A., & Chilamkurti, N. (2017). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems.
6. Khan, M. A., & Salah, K. (2017). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems.
7. Mai J. Big data privacy: The datafication of personal information. Information Society [serial online]. May 2016;32(3):192-199. Available from: Education Source, Ipswich, MA.
8. Michele De D, Nicola D, Alberto G, Angelo S. DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation. Security And Communication Networks, Vol 2018 (2018) [serial online]. 2018;Available from: Directory of Open Access Journals, Ipswich, MA.
9. Smith, S. W., Ph.D. (1997). Chapter 26: Neural Networks (and more!) - Neural Network Architecture. In The Scientist and Engineer's Guide to Digital Signal Processing (3rd ed.). Retrieved from http://www.dspguide.com/ch26/2.htm.
10. Weber, R. H. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1), 23-30. https://doi.org/10.1016/j.clsr.2009.11.008.

IMAGE REFERENCES

1. Financial Tribune. (2017, July 12). File:11_mr_iot_500-ed.jpg [digital image]. Retrieved from https://financialtribune.com/sites/default/files/field/image/17january/11_mr_iot_500-ed.jpg.
2. Glosser.ca. (2013, February 28). File:Colored neural network.svg [digital image]. Retrieved from https://commons.wikimedia.org/wiki/File:Colored_neural_network.svg.