The Internet of Things: Risks and Management

[redacted]

Abstract

The Internet of Things (IoT) is becoming widely popular among the global population with the growth and development of artificial intelligence (AI). IoT offers an extensive amount of benefits that could greatly impact life in terms of convenience, education, health care, and sustainability. With this growth comes a wide range of risks concerning the privacy and safety of those who use and/or are affected by IoT. There have been numerous debates concerning these risks, questioning whether or not IoT is in the best interest of the public. This paper aims at explaining IoT and its uses, as well as describing the risks of using IoT, and thus how governments, businesses, and individuals can manage those risks to continue utilizing IoT. It argues that even though there are potential risks, IoT is imperative for the sustainability of humanity.

Keywords: The Internet of Things, artificial intelligence, risks, risk management, privacy

The Internet of Things: Risks and Management

The Internet of Things is one of the many forms of artificial intelligence (AI) that is growing in terms of popularity and use. The Internet of Things is a system of networks that allow for the connection between devices, such as smartphones and household appliances, as well as large machines, such as planes and submarines. With this spread of digital networks, there has been an increasing amount of tension and worry regarding the potential risks that could come with it. These risks include hacking, exploitation, identity theft, etc. This concern reaches many levels of the societal triangle, from governmental agencies to businesses to individual civilians. These potential risks have become a public outcry regarding the safety and security of the users of IoT, so much so that there have been numerous debates questioning if IoT should continue to evolve and grow. Despite the potential risk, engineers working with AI have not only developed ways to use AI to secure cyber safety, but have also developed numerous ways in which IoT and IoT devices can benefit and improve civilian life in areas such as healthcare, environmental science, and transportation.

Literature Review

Through careful research and literature review, IoT systems will be defined and exemplified. Following are the benefits of IoT systems, the risks that come with these systems, as well as ways in which these risks may be managed.

Benefits of IoT

IoT is a fairly new concept in the AI world. It can be seen as “an emerging communication paradigm that aims at connecting different kinds of objects to the Internet, in order to harvest data” (Meneghello, Calore, Zucchetto, Polese, Zanella, 2019, p. 8182). IoT is typically used in everyday items, linking one device to another, at can be utilized from remote

locations. For example, newer models of appliances allow consumers to activate the appliances, such as espresso machines, using their smartphone without having to be near the appliances. Although IoT offers conveniences such as this, the system is primarily used for its ability to obtain "abundant sensory information to use for intelligent purposes" (Grosz, et al., 2016, p. 9). It "provides advanced connectivity that goes beyond machine-to-machine (M2M) communications and applies to a diversity of protocols, domains, and applications" (Radanliev, et al., 2019, p. 1). The use of IoT creates a wide and endless range of technological opportunities that could benefit massive portions of the global population by offering efficient ways to complete large and exhausting tasks:

> Applications range from monitoring the moisture in a field of crops to tracking the flow of products through a factory, to remotely monitoring patients with chronic illnesses and remotely managing medical devices, such as implanted devices and infusion pumps (Bertino, 2016, p. 1).

Even though IoT can vastly benefit military research, IoT research has been mostly focused on developing ways in which it could improve public safety on a day-to-day basis. These devices can, for example, be used to operate traffic lights and cameras to ensure better timing of traffic, thus reducing car build-up, as well as the number of accidents. IoT can be used in "cameras for surveillance that can detect anomalies pointing to possible crime, drones, and predictive policing applications" (Grosz, et al., 2016, p. 37). In this perspective, IoT may help to drop crime rates by predicting when and where crimes might occur and may help to find suspects at a faster pace using improved systems of face recognition through traffic cameras. It could potentially "prove useful in helping police manage crime scenes or search and rescue events by helping commanders prioritize tasks and allocate resources" (Grosz, et al., 2016, p. 37). With the

rising use of IoT, the term "smart" has been paired in areas through which IoT could greatly benefit: smart cities, smart education, smart healthcare, etc. These concepts refer to the use of IoT in these fields, offering technology that will allow access to a more efficient way of learning, a more accurate way of diagnosing patients, and even a more sustainable way of life. Engineers have been motivated by national issues to create new means to better these areas of life through the use of IoT.

Smart Healthcare

A large chunk of smart healthcare focuses on caring for elderly people. By 2030, it is expected that elderly people will have access to "mobile applications that monitor movement and activities, coupled with social platforms, will be able to make recommendations to maintain mental and physical health," as well as "smart devices in the home will help with daily living activities when needed, such as cooking and, if robot manipulation capabilities improve sufficiently, dressing and toileting" (Grosz et al., 2016, p. 31). There has also been a focus on creating means of easier communication between elderly people and their families; though smartphones currently have easy-communication technologies, such as video-calling, most elderly people are unaware of or simply cannot use these devices, due to the lack of familiarity with the technology. Engineers hope to create simpler devices that allow elderly people the ability to "sharing of information [that] will help families remain engaged with one another at a distance, and predictive analytics may be used to "nudge" family groups toward positive behaviors, such as reminders to "call home," (Grosz, et al., 2016, p. 31).

Smart healthcare also focuses largely on devices that can diagnose patients, as well as devices that can monitor health in more efficient ways than smartwatches. Scientists Zhe Yang, Qihao Zhou, Lei Lei, Kan Zheng, and Wei Xiang have developed the concept of "wearable ECG

monitoring systems" (Yang, et al., 2016, p. 285). ECG refers to an electrocardiogram, which is the monitoring of a person's heartbeat. These scientists argue that because "health conditions of aged people usually need to be checked more frequently" there should be more efficient means "to [identifying] human diseases in a timely and accurate manner with low costs" (Yang, et al., 2016, p. 285) Through the use of the IoT cloud, or the network of shared connections, Yang and his colleagues have developed a means in which the "wearable ECG monitoring" device can "…clean…store…analyze… [and produce a] disease warning" (Yang, et al., 2016, p. 286). This "wearable ECG monitoring" device operates by using a network such as a WiFi router or Bluetooth to connect to either a smart device or computer through an IoT system. This allows for operation and control of the device from even remote locations, allowing doctors and family members to access the information without the interaction between the person wearing the device. The device operates simply using three electrodes stuck onto the skin and

> [through this] wearable monitoring node with three electrodes, real-time ECG signals can be collected with satisfactory accuracy… [though] the accuracy of diagnostic results based on the ECG signal needs to be improved so as to provide a more reliable disease diagnosis. It is believed that long-term and user-friendly ECG monitoring can greatly help mitigate existing healthcare problems to a certain extent (Yang, et al., 2016, p. 294).

Smart Education

Smart education refers to academic learning through the use of technological resources and tools. IoT systems help educators improve academic learning through various means, such as Intelligent Tutoring Systems (ITS). ITS can be implemented through devices such as computers and smartphones, using IoT systems to provide connections between students and educators, even from remote locations. ITS can offer means to things such as "vocabulary,

(who/what/when/where/why) questions, and multiple-choice questions, using electronic resources… and online ontologies" (Grosz, et al., 2016, g. 32). Smart education technologies such as ITS offer opportunities for "cloud computing, learning analytics and big data, which focus on how learning data can be captured, analyzed and directed towards improving learning and teaching, [which] support the development of the personalized and adaptive learning" (Zhu, et al., 2016, g. 1).

Zhu and colleagues define smart education environments in their paper "A research framework of smart education," emphasizing the primary abilities behind the concept. They claim that if a student can master these four abilities, an enriching and effective smart education environment has been implemented. These abilities include: "basic knowledge and core skills, comprehensive abilities, personalized expertise and collective intelligence" (Zhu, et al., 2016, g. 7). They follow this by offering ways in generating and approving upon these abilities, explaining that they can best be achieved through the use of IoT systems. They emphasize the use of

> differentiated instruction [which is a] process to approach teaching and learning for students with different abilities in the same class… collaborative learning [where] two or more people learn or attempt to learn something together… personalized learning [by] adjusting pace, approach, and connecting to the learners' interests and experiences to meet [student needs]… [and] generative learning [which creates and refines] personal mental constructions about the environment (Zhu, et al., 2016, p. 10).

These forms of instruction and learning can be achieved with IoT systems by using various forms of computing, such as "cloud… fog… and swarm" (Zhu, et al., 2016, p. 12-13). These styles of computing focus on the use, storage, and transferring of data through devices that can

interact with IoT systems. The most common technological advancement in smart education using this concept is the e-Textbook; online textbooks offer easy access to texts and often come paired with tools, such as audio translation and definition access. Zhu and her colleagues have also developed the e-schoolbag, which is a collaboration of textbooks and other learning applications accessible through the use of IoT systems. These scientists have found the e-schoolbag to be highly effective in smart learning environments; the "team [was] invited by the Minhang district to design application models of using e-schoolbags in 67 schools since 2012, about seven thousands of students [were] involved" (Zhu, et al., 2016, g. 14). The study continues to expand as the popularity of the e-schoolbag rises.

Smart Cities

Smart cities can be defined as cities using IoT to create effective operations, such as factory production and energy generation. IoT is also used to create safe and efficient means of sharing information with the general public. The focus of smart cities is to improve the overall quality of life through improving government services, thus improving the conditions of citizen life. They also focus on managing resources, with the use of IoT devices, to obtain sustainability. There have been several successes with smart cities. India's government "announced for creation of 100 Smart Cities where the citizens are expected to use Information and Communication Technology with the help of internet" in 2015 through "its policy of Smart City Mission" (Chatterjee, Kar, Gupta, 2018, p. 349). The overall goal was to reduce the costs and time spent completing everyday tasks through the use of IoT devices and technologies. Chatterjee and colleagues have found that the people living in the cities planned for the transformation into smart cities are full of anticipation and eagerness as they will have better access to more effective and wide-range internet. The system designers are currently working on means "to increase [this]

behavior intention and satisfaction of potential users"' they are working towards being 'sincere and honest towards accuracy, understandability, completeness, and security of information" (Chatterjee, et al., 2018, p. 358).

Vulnerabilities associated with IoT Benefits

Though IoT offers a wide range of improvements in not only everyday life but also the improvement of society long term, there is a considerable amount of concern regarding the vulnerabilities IoT is associated with. "Since the IoT initiative is related with generation, storing and exchange of huge data, naturally it is not free from security and privacy vulnerabilities" (Chatterjee, et al., 2018, p. 359). Cybersecurity has become the main concern when accessing all "smart" areas and it is imperative to understand these vulnerabilities and risks to establish the areas in which IoT can be further developed through other forms of AI. Acknowledgment of these risks, as well as the communication of these risks and the plans in which they will be addressed, will help to gain the public's trust in IoT, thus expunging the delay of the benefits IoT can potentially offer to people on a global scale, such as the ones mentioned previously:

> If society approaches these technologies primarily with fear and suspicion, missteps that slow AI's development or drive it underground will result, impeding important work on ensuring safety and reliability of AI technologies (Grosz, et al., 2016, p. 5).

Risks of IoT Systems

Connecting devices and machines through a shared network using the Internet offers an increasing amount of potentially harmful risks as AI continues to develop and expand. The main concern regarding IoT is cybersecurity; because IoT operates on shared networks, cyberattacks can easily be committed because proper safety and security buffers are often disregarded. "…Cybersecurity offense can be expected to increase the number, scale, and diversity of attacks

that can be conducted at a given level of capabilities" (Brundage, et al., 2018, p. 31). Safety and security buffers are often disregarded when it comes to the rising use of smart devices; the security and privacy of its users do not take precedence. It is common for users to purchase "IoT commercial products that are provided with inadequate, incomplete, or ill-designed security mechanisms," leaving room for users to be easily hacked, thus jeopardizing their privacy (Meneghello, et al., 2019, p. 8182). These users are exposed to the possibilities of having their software recoded to allow viruses and other harmful attributes to their devices. In cases such as the "wearable ECG monitoring system," acts such as this can be potentially life-threatening. Users may also experience instances such as hackers using:

> online information… to automatically generate custom malicious websites/emails/links they would be likely to click on, sent from addresses that impersonate their real contacts, using a writing style that mimics those contacts (Brundage, et. al., 2018, p. 24).

Users are even potentially exposed to the possibility of having their identity stolen, as well as money stolen through fraudulent online transfers. Hackers may also utilize a user's device to conduct fraudulent tasks towards other users, thus potentially jeopardizing a user's credibility.

Because IoT covers such a vast range of devices, information can be collected and used against users in various ways; "collected data can indeed range from simple room temperature and humidity measurements, to more sensitive information such as the heart-rate-signal, or the user's location and living habits" (Meneghello, et al., 2019, p. 8183). Such as with the "wearable ECG monitoring system," having information about the "locations and living habits" of a user can potentially put them at risk of physical harm and life-threatening situations. Though this is most common on an individual basis, businesses and smart cities operating through the use of IoT also face the same issues regarding cybersecurity; "…they face strategic, compliance,

operational, financial, and reputational risks regularly, all of which could affect their profitability or ability to function" (Radanlieva, et al. 2019, p. 3).

HP conducted a study examining the amount of "vulnerabilities" in smart devices, finding that there are "25 vulnerabilites…per device"; such vulnerabilities included the lack of complex passwords, "[nonencrypted] local and remote traffic communications," and weak "user interfaces and/or… firmware" (Bertino, 2016, p. 1). Bertino explains that these vulnerabilities in IoT correlate to the fact that IoT devices "do not have well defined perimeters, are highly dynamic, and [are] continuously [changing] because of mobility" (Bertino, 2016, p. 1). Because of these aspects, "IoT systems… may be physically unprotected and/or controlled by different parties," leaving an alarming amount of room to commit cyberattacks "because of the lack of adoption of well-known security techniques, such as encryption, authentication, access control, and role-based control. (Bertino, 2016, p. 1).

Assessment of Risks

It is imperative to understand that the AI technologies, such as IoT, developed by engineers are created (more likely than not) with the notion that they will be used for beneficial use. Though these engineers are aware of the risk that their technologies may be used in harmful manners, "it may not [always] be possible for AI researchers simply to avoid producing research and systems that can be directed towards harmful ends" (Brundage, et al., 2018, p. 16). Despite these risks, it is important to continue to develop and utilize IoT systems for the overall benefit of society; "as a society, we are now at a crucial juncture in determining how to deploy AI-based technologies in ways that promote, not hinder, democratic values such as freedom, equality, and transparency" (Grosz, et al., 2016, p. 6). Achieving safe and secure IoT systems promoting these aspects is possible through correct and effective risk management strategies.

Risk Management

The risk of IoT systems can be managed by many means. The first and foremost would be to provide extensive and adequate information to the public regarding the preventions they can take regarding their IoT systems and devices. With the knowledge of the risks, individuals can take action against cyberattacks by embedding security systems into their IoT systems and devices. Such security systems can be virus protection applications, stronger and complex security passwords, and hacker-detection software. Though these may not eliminate the risks, they will allow for a smaller chance of being hacked:

> AI prediction tools have the potential to provide new kinds of transparency about data and inferences and may be applied to detect, remove, or reduce human bias, rather than reinforcing it (Grosz, 2016, p. 8).

It should be noted here that human bias refers to human presence manipulating IoT systems.

Marwedel and Engel have proposed a new concept for detecting and extracting viruses from AI systems, using a contraption consisting of gold layers and reflective lights, "viruses can get stuck at the gold layer, by binding to the antibodies on top of the gold layer… this change can be detected [thus] viruses can be detected" (Marwedel, Engel, 2016, p. 14). They claim this device can be used efficiently in fast-paced areas, such as businesses and health clinics. Marwedel and Engel also suggest using the "traditional fault-tolerance approach" to detect errors that may allow for cyberattacks; this approach is:

> based on the replication of hardware components. [It relies] on the addition of redundant processing units, using Dual or Triple Modular Redundance, and redundant storage using error correcting codes during a system's lifetime with a high probability of success (Mardwedel, Engel, 2016, p. 21).

Implementing common and global policies through governmental oversight regarding IoT will also help to battle the risks of cyberattacks. Scientists Rodrigo Roman, Cristina Alcaraz, Javier Lopez, and Nicolas Sklavos recommend using key management across all IoT systems and devices to ensure stronger encryption codes (Roman, et al., 2014, p. 147). Aside from this, there should also be a well-defined path concerning the functions and usage of AI technology, including IoT, across the globe. Governmental oversight regarding this path should include "experts who understand and can analyze the interactions between AI technologies, programmatic objectives, and overall societal values" in order to ensure that the functions and usage of AI technology are being used safely and for the benefit of the majority (Grosz, et al., 2016, p. 43). Grosz et. al also advises governments to provide more funding in the AI field in order to obtain more knowledge on how these governments can better protect their citizens from cyberattacks (Grosz et al., 2016, p. 43).

Discussion

IoT systems and devices offer a lot of potential benefits to the majority of the global population. Acknowledging these benefits, as well as the risks, will help the public grasp the concept of IoT and thus prepare them for these risks. It is important to provide honest means of management when regarding these risks so that the public may understand that IoT systems and devices will continue to expand in complexness and usage with careful consideration of the balance between the pros and cons IoT offers. Risks of IoT must continue to be assessed in order to achieve more effective and lasting ways of managing and preventing these risks.

Conclusion

The Internet of Things is a fast-growing form of artificial intelligence that will revolutionize the world for the greater good. By improving areas such as healthcare, education,

and environmental sustainability, IoT offers hope for the future of humanity. As other AI technologies develop, IoT has the potential of becoming exceptionally safe and secure, providing means to tasks that seemed impossible just a decade ago.

Future Direction

In the future, the global population will rely heavily on IoT systems and devices. With effective risk management policies and access to correct information regarding IoT, the population will embrace this ever-growing technology. Modern, mundane, everyday tasks will become a thing of the past. Humanity will rely on this technology to provide not only convenience but also sustainable life.

References

Bertino, E. (2016). Data Security and Privacy in the IoT. *Open Proceedings*, *2*, 1–3.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., & Dafoe, A. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Oxford, England: University of Oxford.

Chatterjee, S., Kar, A. K., & Gupta, M. P. (2018). Success of IoT in Smart Cities in India: An empirical analysis. *Government Information Quarterly*, *35*, 349–361.

Grosz, B. J., Horvitz, A. E., Mackworth, A., Mitchell, T., Mulligan, D., & Shoham, Y. (2016). Artificial Intelligence and Life in 2030: One Hundred Year Study on Artificial Intelligence, 1–40.

Marwedel, P., & Engel, M. (2016). Cyber-Physical Systems: Opportunities, Challenges and (Some) Solutions. In *Management of Cyber Physical Objects in the Future Internet of Things: Methods, Architectures, and Applications* (pp. 1–30). Switzerland: Springer.

Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. *Internet of Things Journal*, *6*(5), 8182–8201.

Radanliev, P. C., De Roure, D. R. C., Maple, C. undefined, Nurse, J. undefined, Nicolescu, R. undefined, & Ani, U. undefined. (2019). *Cyber Risk in IoT Systems*. UK EPSRC.

Roman, R., Alcaraz, C., Lopez, J., & Sklavos, N. (2014). Key management systems for sensor networks in the context of the Internet of Things. *Computers and Electrical Engineering , 37*, 147–159.

Yang, Z., Lei, L., Zheng, K., & Xiang, W. (2016). An IoT-cloud Based Wearable ECG Monitoring System for Smart Healthcare. *Journal of Medical Systems*, *40*, 286–297.

Zhu, Z.-T., Yu, M.-H., & Riezebos, P. (2016). A research framework of smart education. *Smart Learning Environments, 3,* 1–17.