ACTA SCIENTIFIC COMPUTER SCIENCES

Volume 2 Issue 3 March 2020

Research Article

The Internet of Things and Cybersecurity

Cheryl Ann Alexander[1]* and Lidong Wang[2]

[1]*Institute for IT innovation and Smart Health, Mississippi, USA*

[2]*Institute for Systems Engineering Research, Mississippi state university, Vicksburg, USA*

***Corresponding Author:** Cheryl Ann Alexander, Institute for IT Innovation and Smart Health, Mississippi, USA.

Received: February 18, 2020

Published: February 29, 2020

Abstract

The Internet of Things (IoT) is a various collection of interconnected Internet devices such as sensors, smartphones, PCs, wristwatches, etc. These interconnected devices can play an important role in the care of elderly adults with chronic illness, children, communication, and more. However, cybersecurity is critical in the IoT arena because not all are completely secure from hackers and Ransomware, viruses, malware, and other software to steal data and money can compromise sensors, smartphones, PCs, tablets, etc. In this study, we will look at an overview of cybersecurity in IoT and take a special look at how IoT is used in the care of elderly adults and those with special needs and how engineering solutions in IoT can help.

Keywords: Internet of Things; Cybersecurity; Special Needs; Interconnected devices; Sensors

Introduction

The Internet of Things (IoT) is a collection of various interconnected devices which are connected to the Internet and Cloud. These devices can be accentuators, sensors, smartphones, wearables, etc. The devices connected to the IoT generate massive volumes of data and are used in a variety of social, business, government, legal, home, transportation, and healthcare domains [1]. However, there are significant challenges before the full realization of IoT will be achieved in these domains. The primary challenge for implementing total use of IoT is cybersecurity. Data provenance, data integrity, identity management, and privacy are a few of the problems facing IoT devices today [2]. Data security is key in helping IoT reach its full potential, however, today, many hackers attack devices using Ransomware, malware, or other malicious software. The price of personal data has reached an all-time high on the black market today and cybercriminals target those devices easiest to compromise [1].

Currently, society interacts with technology resulting from a major paradigm shift. Computing has become more centered on the rapidly changing technology which captures a massive amount of information and data as individuals and devices connect to the IoT. The purpose of connecting many devices to the IoT is to control actuators. There are millions of devices that are interconnected, including medical implants, appliances, artificial intelligence machines, etc. With this massive number of interconnected devices making data easily available, data security becomes key to prevent unauthorized access to this data [1]. Societal challenges such as car accidents can be tracked using various IoT devices and artificial intelligent robots, however this would also make this data available to third parties who may want to utilize the data negatively. Therefore, cybersecurity becomes the critical challenge in IoT [3].

Key challenges for IoT

Data security, data privacy, and data provenance become the key challenges for users of IoT devices. However, as researchers indicate, a proactive approach is needed to combat this problem because of the widespread use of IoT devices and the lack of interconnected security protocols. Measures to prevent data theft must be implemented to protect the privacy of users' data [1]. Because IoT devices tend to be switched on and connected 24-hours per day, cybercriminals target IoT devices as easily susceptible devices to corrupt. For example, cybercriminals may want to blackmail or spy on someone, steal personal data, install Ransomware, or mine for cryptocurrencies. Not only can these tasks be performed, but cybercriminals can create a botnet with the information they obtain. Therefore, a solid defense mechanism for cybersecurity is necessary to protect valuable data [2].

Botnets are being used in a many phishing campaigns, which are popular among cybercriminals. Other cybercriminals use spam, deliver malware, or conduct Distributed Denial of Service (DDOS) attacks; IoT devices are a huge source of DDOS attacks. The main problem with cybersecurity is that most IoT users do not pay enough attention to preventing attacks or they do not want to spend the money to buy secure software to prevent attacks. Cybercriminal activities will only grow until cybersecurity becomes a priority among smart device users [2]. With smart devices being

used in novel ways, and the pervasive use of smart devices by most homes such as smart appliances, smart lighting, smart baby monitors, etc., cybercriminals can have their choice of ways to affect the personal life of an IoT user [4].

As an example of a problem for IoT device users, cybercriminals can access a smart baby monitor and talk inappropriately and lewdly to the child. Another example would be for a hospital to have their records seized by Ransomware and must pay millions of dollars just to retrieve their data from a cybercriminal. There are many methods of seizing control of a smart device and a user's data; it is imperative that users beware and take proactive responses by installing strong security protocols on all devices. In the home, there are many places a criminal can access data. Strong security should be a priority for every IoT device user [4].

Considerations in IoT

Unfortunately, researchers have failed to consider the user as the primary security component and currently users are considered the weakest link for security. This mistake can be a fatal flaw as the failure to consider the human factor can prove any device to be useless. Therefore, researchers must take an approach which considers the user's safety and the human factor throughout the cybersecurity solution [4]. The primary role of IoT is to connect people with the Internet in many ways and to deliver useful data about the user. Smart cities, smart homes, sensors, smartphones, etc. deliver an interconnected web of devices that connect to the Internet for the user's convenience. This exposure of the user's data to billions of people on the Internet must be carefully guarded to protect the security of the data [3].

There are numerous high capacity devices connected to the IoT that have the capacity to find other devices connected to the IoT and steal data. Although the human factor must be considered, many IoT devices communicate with each other and solutions must consider this, and cybersecurity must provide a strong defensive wall against unwanted intrusion into a user's personal data while connected. It is a well-known fact that many cybercriminals have the capacity to access personal webcams to spy on an individual or even access a baby monitor to spy on a child. It is a confirmed fact that terrorist organizations, criminals, and other nefarious individuals would pay to have access to what the situation may be inside a home, office, or government building. Therefore, it is highly important that cybersecurity solutions take these warnings into consideration and incorporate the human factor into every step of protection [3].

Lack of standards in IoT

The cascading risks of IoT continues to present challenges to individuals in every dimension resulting from the multidimensional nature of IoT. For example, IoT combines cutting-edge technology with big data solutions, distributed data storage, and artificial intelligence (AI). These technologies are highly sensitive to intrusion by spam, malware, Ransomware, and other cybersecurity issues. IoT no longer combines only the consumer product, but considers the product, the algorithm, data, and infrastructure [5].

One example of the lack of cybersecurity standards is the use of IoT in libraries. Privacy safeguards and data interoperability are key concerns for school, city, and university libraries. The need for standards in cybersecurity is obvious so that the full potential of IoT can be realized in library science. As it stands, data is at risk, can be ransomed, or malware installed. Botnets are common attacks in libraries. The change necessary for libraries will require a change in business and economic status, standards, and human interaction. The IoT is currently sensitive to tampering; consider what that means for transportation and safety officials, government offices, and others of critical infrastructure. Cyber-physical systems are also vulnerable to cyberattacks [6].

Because users have not typically been considered when researchers have developed cybersecurity solutions for IoT, a huge missing link has been ignored leading to a continuation of the vulnerability for IoT users. By putting users at ease about what steps are being taken to protect their data, cybersecurity professionals can ensure more efficient standards development and reasonable cybersecurity solutions. Researchers should begin by considering what the users of IoT devices need, their likes and dislikes, and what their respective goals are. Users could be more concerned about what the device can do or how their data is protected. In this case, cybersecurity experts need to meet the needs of the users. Perhaps the user lacks a complete understanding of the risks associated with the use of the IoT device. The user also needs to know his or her role in securing information and protecting data. Putting users at ease is essential in high-level cybersecurity [4]. Expert IoT literature indicates best practices for data provenance and data security. The best practice is that police departments should learn from expert cybersecurity literature [7].

IoT and requirements gathering for individuals with special needs

Requirements gathering is an important part of evaluating how apps can help users with special needs [8]. Accessibility often concerns how well certain third-party apps can assist the disabled with daily tasks. Users with special needs may have problems with sight, hearing, mobility, etc. It can be difficult for individuals with disabilities to make good grades, have a good quality of life, or even live alone [9]. Third-party apps are intended to assist the disabled in having a good quality of life and becoming independent. For example, imagine a student who has poor sight in math class who is unable to see the white board when the instructor writes equations on the board. Figure 1 illustrates the special needs ecosystem along with how disabilities relate to learning [10].

The only time the student gets a chance to see the problems is when handouts are given at the end of class. Imagine an app that

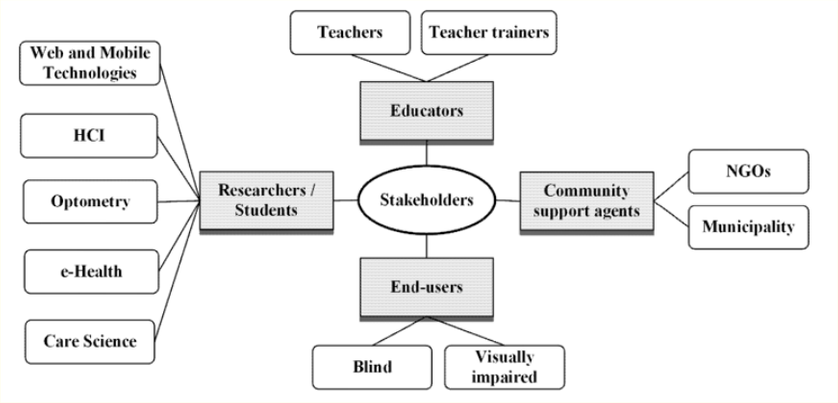

Figure 1: Ecosystem view of the stakeholders.

could help this student get better grades, even excel at math class and connect the problems during the lecture. Requirements gathering is the important part of testing the app's efficiency in doing these things [9].

The widespread portability and use of the Internet and devices connected to the Internet have made it possible for several ways that individuals with disabilities can use apps and tools to assist in daily life. Requirements gathering is the first step in the process to finding these solutions [8,10] have theorized that conventional methods for requirements gathering have failed in gathering information from individuals with special needs due to the limited access and incomprehensiveness of the data gathered. The authors position themselves in favor of using the Internet of Things (IoT) to gather data from various devices so that information is comprehensive and inclusive. By using the IoT, connections to devices such as laptops, tablets, computers, cellphones, sensors, etc. can provide an accurate and complete picture of the needs for individuals with disabilities [8].

Various methods of gathering information

Because understanding of the requirements for individuals with special needs is difficult, and often various methods are used to gather information, the proposed user-centered method is most appropriate. Although current research generally depends on questionnaires, interviews, etc., by using the IoT, data direct from the individual can be collected in real-time and sent directly to researchers. And potential apps can be tested in real-time and responses noted right away because everything is connected to the Internet. People are also using sensors, smartphones, the Internet, etc. daily for almost everything and these devices can capture much data. The IoT is communicating with objects and these objects are sensing data from individuals. Researchers can take advantage of the technologies now available [8].

Ferati, *et al*. take an excellent position in their research article because as technology continues to expand and generate new technologies, these trends offer the researchers a unique opportunity with all the traffic that can be found on the Internet through social media. Websites, sensors, etc. Usability and accessibility are the main reasons why third-party apps and software fail the special needs group. Efforts to only focus on functional requirements and ignoring social and usability requirements elicit higher costs and more time in development [8,10]. Over the last twenty years or so, more and more government agencies have become advocates for those with disabilities and now look for better solutions to development [11].

Ferati, *et al.* have written a comprehensive, well-thought article about using the IoT to aid in the research for individuals with disabilities. As is well-stated in the article, direct communication with the participants is necessary to do good research in this area, there are barriers that limit access to this population, and the IoT is the latest technology allowing real-time data collection and one-to-one communication regarding needs so that software and apps can be developed timely and without much cost [8].

The elderly as a special needs population

With the ever-growing population of elderly, and individuals living longer and fuller lives, sustainable solutions to support independent living for the elderly who have special needs is a priority. From smart homes, fall trackers, and smartphones with GPS trackers, to sensors, and IoT use to provide these solutions, researchers should be able to provide a safe and independent living environment for the elderly with special needs. Because injuries are common among the elderly, with falls being the number one documented injury, solutions that monitor the elderly patient's status while at home is necessary to provide a safe environment. Falls can be the number one cause of injury, death, and dysfunction. Therefore, a solution would be to provide the elderly special needs patient (e.g., blind, dementia, hearing loss, etc.) with sensors and direct real-time communication with healthcare providers in case of a fall. The IoT is an essential part of this plan [12].

Focused research on the elderly and IoT

Researchers have proposed and tested a single-tri-axial accelerometer that attaches to the elderly patient's inner thigh to distinguish between a fall event and activities of daily living (ADLs). The proposed system should have two settings: fast and slow, to detect fall events. In the fast mode, a fall is predicted; for the slow mode, a fall has already occurred [13]. The fast mode has an algorithm and notifies the patient and caregivers prior to the fall. Testing of the sensors indicated the fast and slow modes were 85% accurate in predicting falls [14]. These sensors could mean the difference between quality of life, life, and death for the elderly disabled individual. Independent living is in the best interest of the patient therefore, this fall system should be further developed [13].

To implement the study, a group of elderly disabled individuals who are blind, wishing to live independently, who have suffered frequent falls should be selected. Sensors should be developed using the algorithm and settings and attached for a 90-day period to the test subject. Indoor and outdoor ADLs should be recorded. Patient education is also important, and the patient should be educated on the use of the sensors, etc. The risks that the researcher might encounter is a fall resulting in death, loss of a sensor and undetected falls, and lack of cooperation by the patient or patient's family. The effectiveness of this plan will be evaluated by determining how many falls were predicted accurately and whether or not the individual is able to continue to live independently.

Discussion and Conclusion

The threat from cybercriminals is a reality when using smart devices. The IoT is complete with numerous interconnected devices connected to the Internet. A lack of standards and consideration of the user has left the IoT devices vulnerable to cyberattacks such as malware, spam, Ransomware, etc. Researchers need to develop solutions which consider the user and strong data security protocols. A lack of standardization among cybersecurity professionals contributes to the problem of cyberattacks. It is necessary to take into consideration the examples from reality that have plagued society such as when baby monitors get hijacked and web cameras are hijacked so that criminals can spy on individuals. Also, at risk are the government offices and cyber-physical systems in the United States which rely on IoT for delivery of services.

Acknowledgements

The authors would like to thank Technology and Healthcare Solutions for support.

Conflict of Interest

Any financial interest or any conflict of interest does not exist.

Bibliography

1. Kanuparthi A., *et al*. "Hardware and embedded security in the context of internet of things". In Proceedings of the 2013 ACM workshop on Security, privacy and dependability for cyber vehicles (2013): 61-64.
2. Prokofiev AO., *et al*. "The Internet of Things cybersecurity examination". 2017 Siberian Symposium on Data Science and Engineering (SSDSE), Data Science and Engineering (SSDSE), 2017 Siberian Symposium On (2017): 44.
3. Đekić MD. "The Internet of Things Security". *Tehnika* (2017): 309.
4. Chong I., *et al*. "Human Factors in the Privacy and Security of the Internet of Things". *Ergonomics in Design* 27 (2019): 5-10.
5. Tschider CA. "Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age". *Denver Law Review* 1 (2018): 87.
6. Abo-Seada AA. "The Impact of the Internet of Things on Libraries and Users". *Computers in Libraries* 39.1 (2019): 18-21.
7. Swire P and Woo J. "Privacy and Cybersecurity Lessons at the Intersection of the Internet of Things and Police Body-Worn Cameras". *North Carolina Law Review* 5 (2017): 1475.
8. Ferati M., *et al*. "Augmenting Requirements Gathering for People with Special Needs Using IoT: A Position Paper". 2016 IEEE/ACM Cooperative and Human Aspects of Software Engineering (CHASE), Cooperative and Human Aspects of Software Engineering (CHASE), 2016 IEEE/ACM, CHASE (2016): 48.
9. Ludi S., *et al*. "Requirements gathering for assistive technology that includes low vision and sighted users". 2012 First International Workshop on Usability and Accessibility Focused Requirements Engineering (UsARE), Usability and Accessibility Focused Requirements Engineering (UsARE) (2012).
10. Ferati M., *et al*. "Accessibility requirements for blind and visually impaired in a regional context: An exploratory study". 2014 IEEE 2nd International Workshop on Usability and Accessibility Focused Requirements Engineering (UsARE), Usability and Accessibility Focused Requirements Engineering (UsARE) (2014).
11. Baule SM. "Evaluating the Accessibility of Special Education Cooperative Websites for Individuals with Disabilities". TechTrends: Linking Research and Practice to Improve Learning A Publication of the Association for Educational Communications and Technology 1 (2019).
12. Baig MM., *et al*. "A Systematic Review of Wearable Sensors and IoT-Based Monitoring Applications for Older Adults – a Focus on Ageing Population and Independent Living". *Journal of Medical Systems* 43(2019).
13. Saadeh W., *et al*. "A Patient-Specific Single Sensor IoT-Based Wearable Fall Prediction and Detection System". IEEE Transactions on Neural Systems and Rehabilitation Engineering, Neural Systems and Rehabilitation Engineering, IEEE Transactions on, IEEE Transactions on Neural Systems and Rehabilitation Engineering (2019): 995.

14. Alkhatib S., *et al*. "Privacy and the Internet of Things (IoT) Monitoring Solutions for Older Adults: A Review". Health Informatics Conference, Sydney Australia, 2018. *Studies in Health Technology and Informatics* 252 (2018): 8-14.